

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

GEFAHR

bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

WARNUNG

bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

VORSICHT

mit Warndreieck bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

VORSICHT

ohne Warndreieck bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG

bedeutet, dass ein unerwünschtes Ergebnis oder Zustand eintreten kann, wenn der entsprechende Hinweis nicht beachtet wird.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

WARNUNG

Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Vorwort

Vorwort

Dieses Handbuch...

...unterstützt Sie bei der Projektierung der Security-Funktionalitäten folgender Produkte:

"Security Appliances":

- SCALANCE S: S602/ S612/ S623
- SOFTNET Security Client

"Security Integrated"-Produkte:

- S7-CPs: CP 343-1 Advanced, CP 443-1 Advanced
- PC-CP: CP 1628
- SCALANCE M: SCALANCE M87x und MD74x

Allgemeine Benennung "Security-Modul"

In der vorliegenden Dokumentation werden die folgenden Produkte unter der Benennung "Security-Modul" zusammengefasst: CP 343-1 Advanced, CP 443-1 Advanced, CP 1628, SCALANCE S 602 V3/SCALANCE S 612 V3/SCALANCE S 623 V3.

Funktionsunterschiede werden durch Symbole gekennzeichnet (siehe Abschnitt "Symbolerklärungen"). Hardwarebeschreibungen und Hinweise zur Installation finden Sie in den Dokumenten der einzelnen Baugruppen.

Neu in dieser Ausgabe

In dieser Ausgabe sind unter anderem folgende neuen Funktionen berücksichtigt:

- **Neues Dokumentationskonzept**

Die bisherige Betriebsanleitung "SCALANCE S und SOFTNET Security Client" wird durch ein übergreifendes SIMATIC NET Security-Handbuch abgelöst, das für alle Security-Module gültig ist.

- **Security-Projektierung für SCALANCE S V3.0**

Die Projektierung von SCALANCE S V3.0 Security-Modulen mit neuen Funktionen wird berücksichtigt.

- **Security-Projektierung für CP 343-Advanced, CP 443-1 Advanced**

Zusätzlich zu den SCALANCE S-Modulen kann Security nun auch für die S7 CPs 343-1 Advanced und CP 443-1 Advanced projektiert werden, die in dem vorliegenden Handbuch unter "CP x43-1 Adv." zusammengefasst werden. SCT ist in STEP 7 integriert.

Bisher in STEP 7 verwaltete Benutzer, NTP-Server oder Einträge der IP Access Control Listen können nach SCT migriert werden.

- **Security-Projektierung für CP 1628**

Zusätzlich zu den SCALANCE S-Modulen kann Security nun auch für den PC-CP 1628 konfiguriert werden. SCT ist in STEP 7 integriert.

- **Security Configuration Tool 3.0 - Neue Funktionen**

- Neues Konzept zur Benutzerverwaltung

Neben Benutzern können nun auch Rollen und Rechte angelegt werden. Dabei gibt es systemdefinierte Rollen, die nicht verändert werden können, oder Sie legen neue benutzerdefinierte Rollen an und weisen ihnen Rechte zu.

- Projektweiter Zertifikatsmanager

Zertifikate werden projektübergreifend im Zertifikatsmanager verwaltet.

- Projektweiter NTP-Server

NTP-Server können projektweit angelegt und den einzelnen Modulen zugewiesen. Für CPs wird die gesicherte Uhrzeitübertragung über gesicherte NTP-Server unterstützt.

- Die Konfiguration von SNMPv3 wird unterstützt

- **SOFTNET Security Client V4.0**

- Sie können einen SOFTNET Security Client V4.0 zusammen mit den Security-Modulen konfigurieren und die entsprechenden Konfigurationsdateien erzeugen.

Gültigkeitsbereich dieses Handbuchs

Dieses Handbuch ist für folgende Geräte und Komponenten gültig:

- SIMATIC NET SCALANCE S602 6GK5 602-0BA10-2AA3 - mit FW-Stand ab V3.0
- SIMATIC NET SCALANCE S612 6GK5 612-0BA10-2AA3 - mit FW-Stand ab V3.0
- SIMATIC NET SCALANCE S623 6GK5 623-0BA10-2AA3 - mit FW-Stand ab V3.0
- CP 343-1 Advanced 6GK7 343-1GX31-0XE0 - mit FW-Stand ab V3.0
- CP 443-1 Advanced 6GK7 443-1GX30-0XE0 - mit FW-Stand ab V3.0
- CP 1628 6GK1162-8AA00 - mit FW-Stand ab V1.0
- SIMATIC NET SOFTNET Security Client 6GK1 704-1VW04-0AA0 - Ausgabestand ab 4.0
- Security Configuration Tool - Ausgabestand V3.0

Leserkreis

Dieses Handbuch wendet sich an Personen, welche die Industrial Ethernet Security-Funktionalitäten in einem Netzwerk durchführen.

CP-Dokumentation auf der Manual Collection (Bestell-Nr. A5E00069051)

Jedem S7-CP liegt die SIMATIC NET Manual Collection bei. Diese DVD wird in regelmäßigen Abständen aktualisiert; sie enthält die zum Erstellungszeitpunkt aktuellen Gerätehandbücher und Beschreibungen.

Siehe auch

/7/ (Seite 219)

In dieser Anleitung verwendete Symbole

 S ≥ V3.0

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S ab V3.0 relevant.

 SCA.

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S relevant.

 S602

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Security-Module außer SCALANCE S 602 relevant.

 S623

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für SCALANCE S 623 relevant.

 S7-CP

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für S7-CPs relevant.

 S7-CP

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Security-Module außer den S7-CPs relevant.

 PC-CP

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist nur für PC-CPs relevant.

 PC-CP

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Security-Module außer den PC-CPs relevant.

 CP

Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle S7-CPs und PC-CPs relevant.



Das beschriebene Kapitel / der beschriebene Abschnitt / die beschriebene Zeile ist für alle Security-Module außer den CPs relevant.



Auf besondere Tipps werden Sie in dieser Anleitung mit diesem Symbol hingewiesen.



Das Symbol verweist auf besondere Literaturempfehlungen.



Dieses Symbol weist auf detailliertere Hilfestellung in der kontextabhängigen Hilfe hin. Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

Literaturhinweise /.../

Hinweise auf weitere Dokumentationen sind mit Hilfe von Literaturnummern in Schrägstrichen /.../ angegeben. Anhand dieser Nummern können Sie dem Literaturverzeichnis am Ende des Handbuchs den Titel der Dokumentation entnehmen.

Siehe auch

<http://support.automation.siemens.com/WW/view/de/> ([Support](#))

SIMATIC NET Glossar

Erklärungen zu den Fachbegriffen, die in dieser Dokumentation vorkommen, sind im SIMATIC NET-Glossar enthalten.

Sie finden das SIMATIC NET-Glossar hier:

- SIMATIC NET Manual Collection
Die DVD liegt einigen SIMATIC NET-Produkten bei.
- Im Internet unter folgender Beitrags-ID:
50305045 (<http://support.automation.siemens.com/WW/view/de/50305045>)

Inhaltsverzeichnis

	Vorwort	3
1	Einführung und Grundlagen	13
1.1	Wichtige Hinweise	13
1.2	Einführung und Grundlagen	15
1.3	Produkteigenschaften	16
1.3.1	Funktionsübersicht	16
1.3.2	Mengengerüste	18
1.3.3	Baugruppe austauschen	19
1.4	Einsatz vom SOFTNET Security Client	20
1.5	Einsatz von SCALANCE S602	21
1.6	Einsatz von SCALANCE S612 und S623	23
1.7	Einsatz von SCALANCE S623 - DMZ-Port	26
1.8	Einsatz von CP 343-1 Advanced und CP 443-1 Advanced	27
1.9	Einsatz von CP 1628	31
1.10	Projektierung und Administration	34
2	Projektierung mit Security Configuration Tool	35
2.1	Funktionsumfang und Arbeitsweise	35
2.2	Installation	37
2.2.1	Unterstützte Betriebssysteme	37
2.3	Bedienoberfläche und Menübefehle	38
2.4	Projekte anlegen und verwalten	43
2.4.1	Security Configuration Tool Standalone	43
2.4.2	Security Configuration Tool in STEP 7	43
2.4.3	STEP 7-Daten migrieren	47
2.4.4	Übersicht	49
2.4.5	Initialisierungswerte für ein Projekt festlegen	52
2.4.6	Konsistenzprüfungen	52
2.4.7	Symbolische Namen für IP-/MAC-Adressen vergeben	53
2.5	Konfigurationsdaten für SCALANCE M	56
2.6	Benutzer verwalten	58
2.6.1	Übersicht zur Benutzerverwaltung	58
2.6.2	Benutzer anlegen	59
2.6.3	Rollen anlegen	60
2.6.4	Rechte verwalten	62
2.7	Zertifikate verwalten	66
2.7.1	Übersicht	66
2.7.2	Zertifikate erneuern	68

2.7.3	Zertifikate ersetzen.....	70
3	Module anlegen und Netzparameter einstellen.....	71
3.1	Parameter im Inhaltsbereich	75
3.2	Schnittstellen konfigurieren (SCALANCE S).....	77
3.2.1	Übersicht Ports.....	77
3.2.2	Schnittstellen	78
3.2.3	Dynamisches DNS	80
3.2.4	Porteinstellungen	84
3.2.5	Internetverbindung	85
4	Firewall projektieren.....	87
4.1	CPs im Standard Modus	88
4.1.1	CP x43-1-Advanced	89
4.1.1.1	Voreinstellung der Firewall.....	89
4.1.1.2	Firewall projektieren	92
4.1.1.3	Zugriffsliste projektieren	93
4.1.1.4	Eintrag zur Zugriffsliste hinzufügen.....	95
4.1.2	CP 1628	95
4.1.2.1	Voreinstellung der Firewall.....	95
4.1.2.2	Firewall projektieren	98
4.2	SCALANCE S im Standard Modus	99
4.2.1	Voreinstellung der Firewall.....	99
4.2.2	Firewall projektieren ≥ V3.0	102
4.2.3	Firewall projektieren < V3.0	104
4.3	Im Erweiterten Modus	106
4.3.1	Firewall projektieren	106
4.3.2	Globale Firewall-Regeln.....	107
4.3.2.1	Globale Firewall-Regelsätze - Vereinbarungen	109
4.3.2.2	Globale Firewall-Regelsätze einstellen und zuweisen.....	109
4.3.3	Benutzerspezifische Firewall-Regeln.....	110
4.3.3.1	Benutzerspezifische Firewall-Regeln einstellen und zuweisen	111
4.3.4	Verbindungsbezogene automatische Firewall-Regeln	112
4.3.5	Lokale IP-Paketfilter-Regeln einstellen	114
4.3.6	IP-Paketfilter-Regeln	116
4.3.7	IP-Dienste definieren.....	121
4.3.8	ICMP-Dienste definieren	122
4.3.9	MAC-Paketfilter-Regeln einstellen	124
4.3.10	MAC-Paketfilter-Regeln	125
4.3.11	MAC-Dienste definieren	128
4.3.12	Dienstgruppen einrichten	130
5	Weitere Moduleigenschaften projektieren.....	133
5.1	Security-Modul als Router.....	133
5.1.1	Übersicht	133
5.1.2	Standard-Router.....	134
5.1.3	NAT/NAPT-Routing	135
5.1.4	Adressumsetzung mit NAT/NAPT	137
5.1.5	Zusammenhang zwischen NAT/NAPT-Router und Firewall.....	140
5.1.6	1:1 NAT-Routing - Beispiele zur Konfiguration Teil 1	141
5.1.7	NAT/NAPT-Routing - Beispiele zur Konfiguration Teil 2.....	142

5.1.8	NAT/NAPT-Routing - Beispiele zur Konfiguration Teil 3	144
5.2	Security-Modul als DHCP-Server	147
5.2.1	Übersicht	147
5.2.2	DHCP-Server konfigurieren	149
5.3	Zeitsynchronisierung	153
5.3.1	Übersicht	153
5.3.2	Uhrzeitführung konfigurieren	154
5.3.3	Eintrag hinzufügen	155
5.3.4	NTP-Server definieren	155
5.4	SNMP	157
5.4.1	Übersicht	157
5.4.2	SNMP aktivieren	158
5.5	Proxy-ARP	159
6	Gesicherte Kommunikation im VPN über IPsec-Tunnel	161
6.1	VPN mit Security-Modulen	161
6.2	Authentifizierungsmethoden	164
6.3	VPN-Gruppen	165
6.3.1	Betriebsarten von VPN-Gruppen	165
6.3.2	Gruppen anlegen und Module zuordnen	166
6.4	Tunnelkonfiguration im Standard Modus	169
6.5	Tunnelkonfiguration im Erweiterten Modus	169
6.5.1	Gruppeneigenschaften projektieren	170
6.5.2	Security-Modul in konfigurierte Gruppe aufnehmen	173
6.5.3	Modulspezifische VPN-Eigenschaften konfigurieren	176
6.6	Interne Netzknoten konfigurieren	179
6.6.1	Arbeitsweise des Lernmodus	180
6.6.2	Anzeige der gefundenen internen Netzknoten	182
7	SOFTNET Security Client	185
7.1	Einsatz des SOFTNET Security Client	185
7.2	Installation und Inbetriebnahme des SOFTNET Security Client	188
7.2.1	SOFTNET Security Client installieren und starten	188
7.2.2	SOFTNET Security Client deinstallieren	189
7.3	Konfigurationsdatei mit Projektierwerkzeug Security Configuration Tool erstellen	189
7.4	SOFTNET Security Client bedienen	192
7.5	Tunnel einrichten und bearbeiten	194
8	Online Funktionen - Test, Diagnose und Logging	203
8.1	Funktionsübersicht Online-Dialog	204
8.2	Ereignisse aufzeichnen (Logging)	206
8.2.1	Lokales Logging - Einstellungen in der Konfiguration	207
8.2.2	Netzwerk Syslog - Einstellungen in der Konfiguration	211
8.2.3	Projektierung des Paket-Logging	214

A	Anhang	215
A.1	DNS-Konformität	215
A.2	Wertebereiche IP-Adresse, Subnetzmaske und Adresse des Netzübergangs	215
A.3	MAC-Adresse	216
B	Literaturverzeichnis.....	217
B.1	Einleitung.....	217
B.2	S7-CPs / Zur Projektierung, Inbetriebnahme und Nutzung des CP.....	217
B.2.1	/1/	217
B.2.2	/2/	218
B.3	Zur Projektierung mit STEP 7 / NCM S7.....	218
B.3.1	/3/	218
B.3.2	/4/	218
B.3.3	/5/	219
B.4	S7-CPs Zur Montage und Inbetriebnahme des CP	219
B.4.1	/6/	219
B.5	Zu Aufbau und Betrieb eines Industrial Ethernet-Netzes.....	219
B.5.1	/7/	219
B.6	SIMATIC- und STEP 7-Grundlagen.....	220
B.6.1	/8/	220
B.6.2	/9/	220
B.7	Industrielle Kommunikation Band 2	220
B.7.1	/10/	220
B.8	Zur Konfiguration von PC-Stationen / PGs	221
B.8.1	/11/	221
B.9	Zur Konfiguration von PC-CPs.....	221
B.9.1	/12/	221
B.10	SIMATIC NET Industrial Ethernet Security	221
B.10.1	/13/	221
B.10.2	/14/	222
B.10.3	/15/	222
	Index.....	223

Einführung und Grundlagen

Security-Hinweise

ACHTUNG
Siemens bietet für sein Automatisierungs- und Antriebsproduktportfolio IT-Security-Mechanismen, um einen sicheren Betrieb der Anlage/Maschine zu unterstützen. Unsere Produkte werden auch unter dem Gesichtspunkt IT-Security ständig weiterentwickelt. Wir empfehlen Ihnen daher, dass Sie sich regelmäßig über Aktualisierungen und Updates unserer Produkte informieren und nur die jeweils aktuellen Versionen bei sich einsetzen. Informationen dazu finden Sie unter: http://support.automation.siemens.com Hier können Sie sich für einen produktspezifischen Newsletter registrieren. Für den sicheren Betrieb einer Anlage/Maschine ist es darüber hinaus jedoch notwendig, die Automatisierungskomponenten in ein ganzheitliches IT-Security-Konzept der gesamten Anlage/Maschine zu integrieren, das dem aktuellen Stand der IT-Technik entspricht. Hinweise hierzu finden Sie unter: http://www.siemens.com/industrialsecurity Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen.

1.1 Wichtige Hinweise

Allgemein

ACHTUNG
Schutz vor unberechtigtem Zugriff Achten Sie darauf, dass der Projektierungsrechner und PC/PG bzw. das Projekt vor unberechtigtem Zugriff geschützt ist.

ACHTUNG
Gastkonto deaktivieren Stellen Sie sicher, dass das Gastkonto auf dem Projektierungsrechner deaktiviert ist.

ACHTUNG
Aktuelles Datum und aktuelle Uhrzeit auf den Security-Modulen Achten Sie bei der Verwendung von gesicherter Kommunikation (z. B. HTTPS, VPN...) darauf, dass die betroffenen Security-Module über die aktuelle Uhrzeit und das aktuelle Datum verfügen. Die verwendeten Zertifikate werden sonst als nicht gültig ausgewertet und die gesicherte Kommunikation funktioniert nicht.

Hinweis

Aktuelle Antiviren-Software

Es wird empfohlen, dass auf allen Projektierungsrechnern immer eine aktuelle Antiviren-Software installiert ist.

Hinweis

FTPS

Wird in der vorliegenden Dokumentation die Benennung "FTPS" verwendet, ist damit FTPS im expliziten Modus gemeint (FTPES).

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen. Das Umschalten in den erweiterten Modus ist eine projektweite Einstellung und gilt daher für alle Baugruppen des Projektes.

Abhilfe für SCT Standalone: Sie schließen das Projekt ohne zu speichern und öffnen es erneut.

CP x43-1 Advanced

ACHTUNG

Zusätzliche Sicherheitseinstellungen

Um zu vermeiden, dass unautorisierte Projektierungsdaten in den CP geladen werden, müssen Sie zusätzliche Sicherheitseinstellungen an der Firewall des CPs (Blocken der S7-Kommunikation oder nur getunnelte Kommunikation) vornehmen bzw. externe Sicherheitsmaßnahmen ergreifen.

STEP 7

Hinweis

"Speichern und Übersetzen" nach Änderungen

Damit die Security-Einstellungen in die entsprechenden (Offline-)Systemdatenbausteine übernommen werden, wählen Sie nach vorgenommenen Änderungen das Menü "Station" > "Speichern und Übersetzen" in HW Konfig bzw. "Netz" > "Speichern und Übersetzen" in NetPro.

Hinweis

Öffnen einer Station bei geöffnetem Security Configuration Tool

Schließen Sie das Security Configuration Tool, bevor Sie eine weitere Station über den SIMATIC Manager oder Net Pro öffnen.

1.2 Einführung und Grundlagen

Mit den SIMATIC NET Security-Modulen und dem SIMATIC NET SOFTNET Security Client haben Sie sich für das SIEMENS Sicherheitskonzept entschieden, das den hohen Anforderungen geschützter Kommunikation in der industriellen Automatisierungstechnik gerecht wird.

Hinweis

Aktuelle Antiviren-Software

Es wird empfohlen, dass auf allen Projektierungsrechnern immer eine aktuelle Antiviren-Software installiert ist.

Dieses Kapitel gibt Ihnen einen Überblick über die Sicherheitsfunktionen der Geräte und Komponenten:

- SCALANCE S
- CP x43-1 Advanced
- CP 1628
- SOFTNET Security Client

Tipp:

Den schnellen Einstieg mit den Security-Modulen finden Sie im Dokument "SIMATIC NET Security - Getting Started".



1.3 Produkteigenschaften

1.3.1 Funktionsübersicht

Funktionsübersicht der Gerätetypen

Entnehmen Sie der folgenden Tabelle, welche Funktionen die einzelnen Security-Module unterstützen.

Hinweis

In diesem Handbuch werden alle Funktionen beschrieben. Berücksichtigen Sie anhand der nachfolgenden Tabelle, welche Funktionen auf das von Ihnen genutzte Security-Modul zutreffen.

Achten Sie auch auf die zusätzlichen Angaben in den Kapitelüberschriften.

Tabelle 1- 1 Funktionsübersicht

Funktion	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V3.0
Projektierung über			
Security Configuration Tool	-	-	x
Security Configuration Tool in STEP 7 integriert	x	x	x
Kompatibilität zu			
Anderen Security-Modulen	x	x	x
IP Access Control-Listen (ACL)	x	-	-
SOFTNET Security Client	x	x	x 
Allgemein			
NAT/NAPT-Router	x	-	x
DHCP-Server	-	-	x
Firewall			

Funktion	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V3.0
Lokale Firewall-Regeln	x	x	x
Globale Firewall-Regeln	x	x	x
Benutzerspezifische Firewall-Regeln	-	-	x
IPsec			
Aufbau von IPsec-Tunneln	x	x	x 
Benutzerverwaltung			
Projektierung der Benutzerverwaltung	x	x	x
Migration der aktuellen Benutzerverwaltung	x	-	-
Gesicherte Protokolle			
SNMPv3	x	x	x
HTTPS	x	-	x
FTPS-Server	x	-	-
FTPS-Client	x	-	-
NTP	x	x	x
Gesichertes NTP	x	x	-
Sonstige Protokolle			
PPPoE-Client	-	-	x
DynDNS	-	-	x
Logging			
Aufzeichnung von System-Ereignissen	x	x	x
Aufzeichnung von Audit-Ereignissen	x	x	x
Aufzeichnung von Paketfilter-Ereignissen	x	x	x
Audit-Meldungen in den Diagnosepuffern des Security-Moduls	x	x	-
Zugriff über Security Configuration Tool auf Log-Puffer des Security-Moduls	x	x	x
Web-Diagnose	x	-	-
VPN-Diagnose über Security Configuration Tool (VPN=Virtual Private Network)	x	x	x
Senden der Meldungen an Syslog-Server	x	x	x

x Funktion wird unterstützt

- Funktion wird nicht unterstützt

1.3.2 Mengengerüste

Hinweis

Eine komplette Übersicht der zulässigen Mengengerüste finden Sie im Internet unter folgender Adresse: <http://support.automation.siemens.com/WW/view/de/58217657> (<http://support.automation.siemens.com/WW/view/de/58217657>).

Mengengerüste

Funktion	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V3.0
VPN-Tunnel pro Security-Modul	Max. 16 *		Max. 128
Firewall-Regeln pro Security-Modul	Max. 256		
Projektweit anlegbare NTP-Server (zuweisbare NTP-Server pro Security-Modul)	32 (4)		

* Ab SCT V3.1 geplant:

- Max. 32 für CP x43-1 Adv.
- Max. 64 für CP 1628

Welche Regeln gelten für Benutzernamen, Rollennamen und Passwörter?

Beachten Sie beim Anlegen oder Ändern eines Benutzers, einer Rolle oder eines Passworts die folgenden Regeln:

Erlaubte Zeichen	0123456789 A...Z a...z !"#\$%&'()*+,-./:;<=>?@ [] _ { } ~ ^ `
Länge des Benutzernamens	1 ... 32 Zeichen
Länge des Passworts	8 ... 32 Zeichen
Länge des Rollennamens	1 ... 32 Zeichen
Maximale Benutzeranzahl pro Projekt	128
Maximale Benutzeranzahl auf einem Security-Modul	32 + 1 Administrator beim Anlegen des Projekts
Maximale Rollenanzahl pro Projekt	121 benutzerdefinierte + 4 systemdefinierte
Maximale Rollenanzahl auf einem Security-Modul	37

1.3.3 Baugruppe austauschen



So erreichen Sie diese Funktion

1. Markieren Sie das zu bearbeitende Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Modul austauschen...".
3. Abhängig vom Produkttyp des gewählten Moduls können Sie in dem Dialog den Baugruppentyp und/oder das Firmwarerelease anpassen.

Entnehmen Sie der nachfolgenden Tabelle, welche Module Sie ohne und mit eventuellen Datenverlusten austauschen können.

Hinweis

Ersetzen von Baugruppen unterschiedlichen Typs

- Um eine Baugruppe durch einen anderen Baugruppentyp zu ersetzen, müssen Sie ein neues Modul anlegen und dieses entsprechend konfigurieren.
- Informationen zum Ersetzen von CPs finden Sie im jeweiligen Gerätehandbuch.

Tabelle 1- 2 Kompatible Baugruppen

Ausgangsmodul	Möglicher Baugruppentausch	
	ohne Verluste	mit eventuellen Verlusten
S602 V2 und V3	S612 V2 S613 V2	S612 V1 S613 V1
S612 V1	S612 V2 S613 V1 S613 V2	S602 V2 und V3
S612 V2	S613 V2 S612 V3 S623 V3	S602 V2 und V3 S612 V1 S613 V1
S613 V1	S613 V2 S612 V3 S623 V3	S602 V2 und V3 S612 V1 S612 V2
S613 V2	S612 V3 S623 V3	S602 V2 und V3 S612 V1 S612 V2 S613 V1
SOFTNET Security Client 2005	SOFTNET Security Client 2008 SOFTNET Security Client V3.0 SOFTNET Security Client V4.0	-

Ausgangsmodul	Möglicher Baugruppentausch	
	ohne Verluste	mit eventuellen Verlusten
SOFTNET Security Client 2008	SOFTNET Security Client 2005 * SOFTNET Security Client V3.0 SOFTNET Security Client V4.0	-
SOFTNET Security Client V3.0	SOFTNET Security Client 2005 * und ** SOFTNET Security Client 2008 **	-
SOFTNET Security Client V4.0	SOFTNET Security Client 2005 * und ** SOFTNET Security Client 2008 ** SOFTNET Security Client V3.0	-
SCALANCE M	-	-

* Wenn sich das Modul nicht in einer Routing-Gruppe befindet.

** Wenn sich das Modul nicht mit einem MD-Modul in einer VPN-Gruppe befindet.

Siehe auch

Bedienoberfläche und Menübefehle (Seite 38)

/2/ (Seite 218)

1.4 Einsatz vom SOFTNET Security Client

PG/PC-Kommunikation im VPN - Aufgabe des SOFTNET Security Client

Mit der PC-Software SOFTNET Security Client sind gesicherte Fernzugriffe vom PG/PC auf Automatisierungsgeräte, die durch Security-Module geschützt sind, über öffentliche Netze hinweg möglich.

Mittels des SOFTNET Security Client wird ein PG/PC automatisch so konfiguriert, dass er eine gesicherte IPsec-Tunnelkommunikation im VPN (Virtual Private Network) zu einem oder mehreren Security-Modulen aufbauen kann.

PG/PC-Applikationen wie NCM Diagnose oder STEP 7 können so über eine gesicherte Tunnelverbindung auf Geräte oder Netzwerke zugreifen, die sich in einem durch Security-Module geschützten internen Netz befinden.

Die PC-Software SOFTNET Security Client wird ebenfalls mit dem Projektierwerkzeug Security Configuration Tool konfiguriert; damit ist eine durchgängige Projektierung gewährleistet.

1.5 Einsatz von SCALANCE S602

Firewall und Router - Aufgabe von SCALANCE S602

Durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall und NAT/NAPT-Router schützt das Gerät SCALANCE S602 einzelne Geräte oder auch ganze Automatisierungszellen vor:

- Datenspionage
- unberechtigten Zugriffen

SCALANCE S602 ermöglicht diesen Schutz flexibel und ohne komplizierte Handhabung.

SCALANCE S602 wird mit dem Projektierwerkzeug Security Configuration Tool konfiguriert.

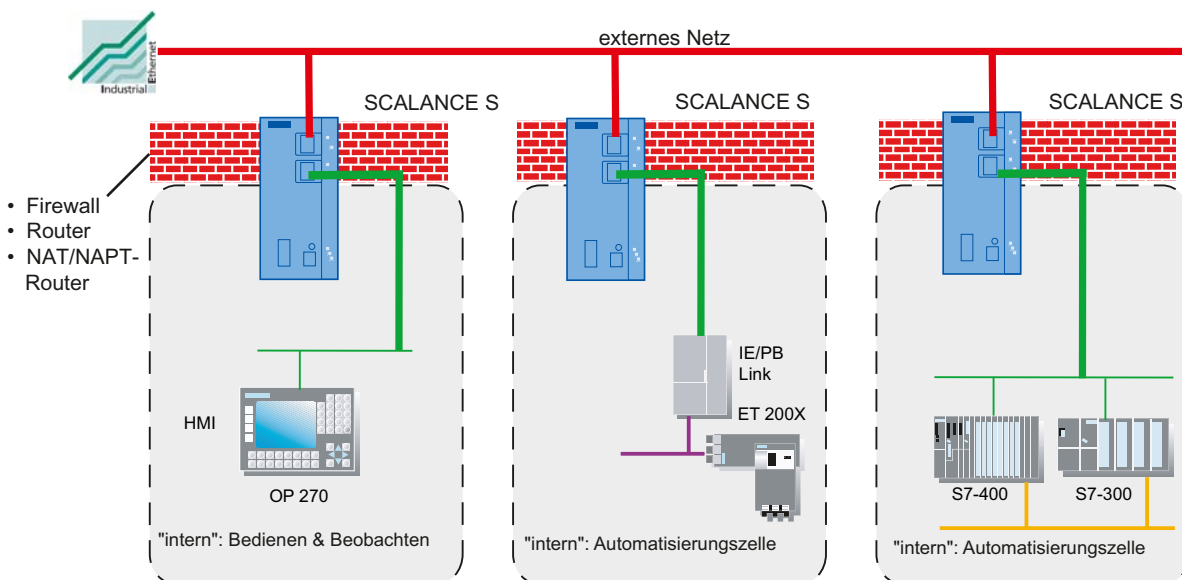


Bild 1-1 Netzkonfiguration mit SCALANCE S602

Sicherheitsfunktionen

- Firewall
 - IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
 - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer-2-Telegramme; gilt nicht für S602, wenn der Router-Betrieb genutzt wird);
 - Bandbreitenbegrenzung

Alle Netzknoten, die sich im internen Netzsegment eines SCALANCE S befinden, werden durch dessen Firewall geschützt.

- Router-Betrieb

Indem Sie SCALANCE S als Router betreiben, entkoppeln Sie das interne Netz vom externen Netz. Das von SCALANCE S verbundene interne Netz wird somit zu einem eigenen Subnetz; SCALANCE S muss als Router explizit über seine IP-Adresse adressiert werden.

- Schutz für Geräte und Netzsegmente

Die Schutzfunktion Firewall kann sich über den Betrieb einzelner Geräte, mehrerer Geräte wie auch ganzer Netzsegmente erstrecken.

- Rückwirkungsfreiheit beim Einbau in flache Netze (Bridge-Betrieb)

Beim Einbau eines SCALANCE S602 in eine bestehende Netzinfrastruktur müssen die Endgeräte nicht neu eingestellt werden.

Interne und Externe Netzknoten :

SCALANCE S602 teilt Netzwerke in zwei Bereiche auf:

- internes Netz: geschützte Bereiche mit den "internen Knoten"

Interne Knoten sind alle diejenigen Knoten, die von einem SCALANCE S abgesichert sind.

- externes Netz: ungeschützte Bereiche mit den "externen Knoten"

Externe Knoten sind alle Knoten, die sich außerhalb der geschützten Bereiche befinden.

ACHTUNG

Die internen Netze werden als sicher (vertrauenswürdig) betrachtet.

Verbinden Sie ein internes Netzsegment nur über SCALANCE S mit den externen Netzsegmenten.

Weitere Verbindungswege zwischen dem internen und externen Netz dürfen nicht vorhanden sein!

1.6 Einsatz von SCALANCE S612 und S623

Umfassender Schutz - Aufgabe von SCALANCE S612 und SCALANCE S623

Durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall, NAT/NAPT-Router und VPN (Virtual Private Network) über IPsec-Tunnel schützen die Security-Module SCALANCE S612 und SCALANCE S623 einzelne Geräte oder auch ganze Automatisierungszellen vor:

- Datenspionage
- Datenmanipulation
- unberechtigten Zugriffen

SCALANCE S ermöglicht diesen Schutz flexibel, rückwirkungsfrei, protokollunabhängig (ab Layer-2 gemäß IEEE 802.3) und ohne komplizierte Handhabung.

SCALANCE S und SOFTNET Security Client werden mit dem Projektierwerkzeug Security Configuration Tool konfiguriert.

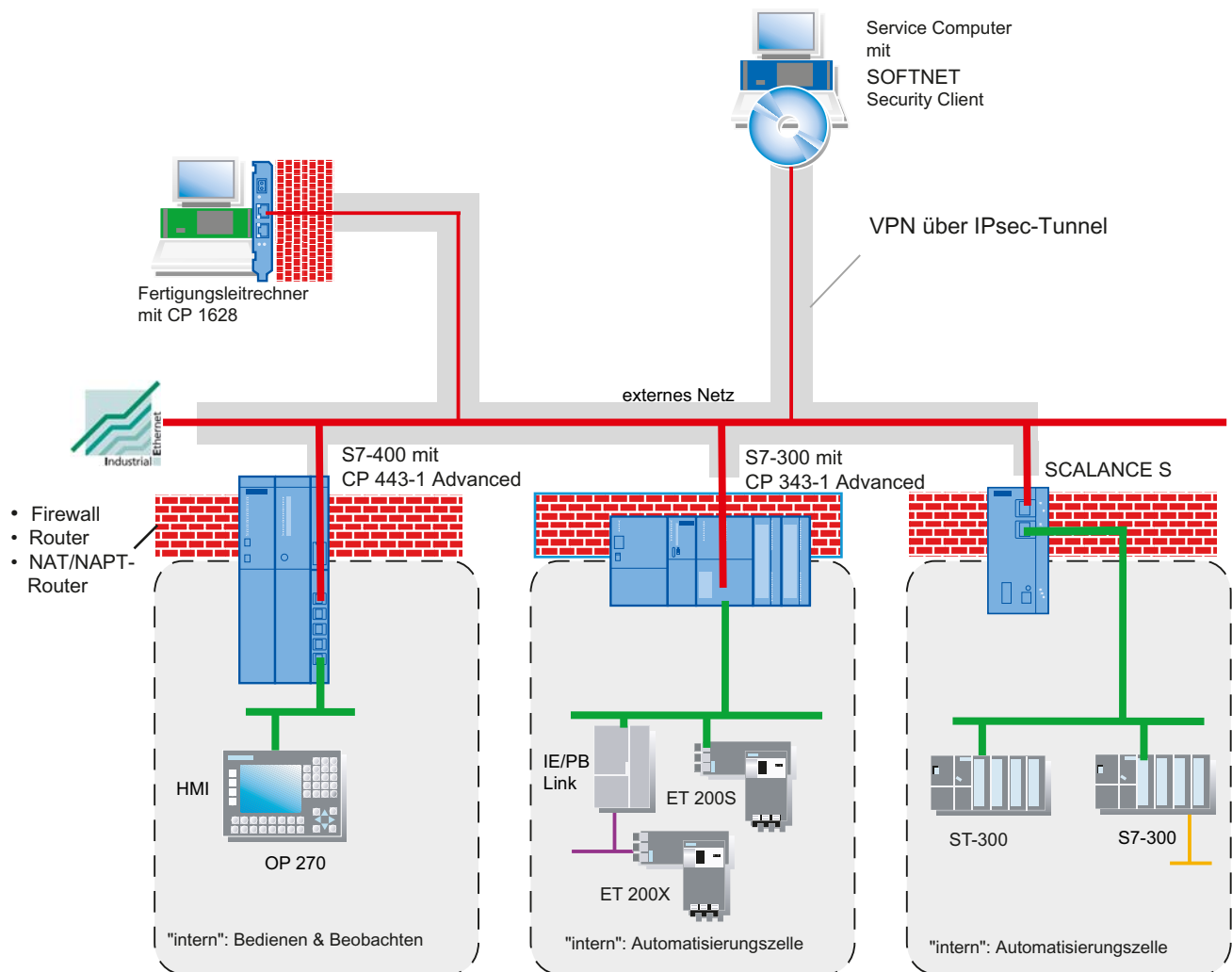


Bild 1-2 Netzkonfiguration mit SCALANCE S612

Sicherheitsfunktionen

- Firewall
 - IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
 - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer-2-Telegramme; gilt nicht, wenn der Router-Betrieb genutzt wird)
 - Bandbreitenbegrenzung
 - Globale und benutzerspezifische Firewall-Regeln

Alle Netzknoten, die sich im internen Netzsegment eines SCALANCE S befinden, werden durch dessen Firewall geschützt.
- Gesicherte Kommunikation durch IPsec-Tunnel

SCALANCE S kann mit anderen Security-Modulen per Projektierung zu Gruppen zusammengefasst werden. Zwischen allen Security-Modulen einer Gruppe werden IPsec-Tunnel aufgebaut (VPN, Virtual Private Network). Alle internen Knoten dieser SCALANCE S können mittels dieser Tunnel gesichert miteinander kommunizieren.
- Protokollunabhängigkeit

Die Tunnelung umfasst auch Ethernet-Telegramme gemäß IEEE 802.3 (Layer-2-Telegramme; gilt nicht, wenn der Router-Betrieb genutzt wird).

Durch die IPsec-Tunnel werden sowohl IP-, als auch Non-IP-Telegramme übertragen.
- PPPoE

Point to Point Protocol over Ethernet (RFC 2516) zum automatischen Bezug von IP-Adressen vom Provider, so dass der Einsatz eines separaten DSL-Routers entfallen kann.
- DynDNS

Dynamischer Domain Name Service zur Verwendung dynamischer IP-Adressen, wenn ein SCALANCE S bei Fernwartungsszenarien als VPN-Server eingesetzt wird.
- SNMPv3

Zur abhörsicheren Übertragung von Netzwerkanalyseinformationen.
- Router-Betrieb

Indem Sie SCALANCE S als Router betreiben, verbinden Sie das interne Netz mit dem externen Netz. Das über SCALANCE S verbundene interne Netz wird somit zu einem eigenen Subnetz.
- Schutz für Geräte und Netzsegmente

Die Schutzfunktion Firewall und VPN kann sich über den Betrieb einzelner Geräte, mehrerer Geräte wie auch ganzer Netzsegmente erstrecken.

- Zusätzlicher DMZ-Port **S623**

- Rückwirkungsfreiheit beim Einbau in flache Netze (Bridge-Betrieb)

Interne Netzknoten können ohne Projektierung gefunden werden. Beim Einbau eines SCALANCE S in eine bestehende Netzinfrastruktur müssen daher die Endgeräte nicht neu konfiguriert werden.

Das Modul versucht interne Teilnehmer zu finden; interne Teilnehmer, die auf diesem Weg nicht gefunden werden können, müssen dennoch projektiert werden.

Interne und Externe Netzknoten:

SCALANCE S teilt Netzwerke in zwei Bereiche auf:

- internes Netz: geschützte Bereiche mit den "internen Knoten"

Interne Knoten sind alle diejenigen Knoten, die von einem SCALANCE S abgesichert sind.

- externes Netz: ungeschützte Bereiche mit den "externen Knoten"

Externe Knoten sind alle Knoten, die sich außerhalb der geschützten Bereiche befinden.

ACHTUNG

Die internen Netze werden als sicher (vertrauenswürdig) betrachtet.

Verbinden Sie ein internes Netzsegment nur über SCALANCE S mit den externen Netzsegmenten.

Weitere Verbindungswege zwischen dem internen und externen Netz dürfen nicht vorhanden sein.

1.7 Einsatz von SCALANCE S623 - DMZ-Port

Zusätzliche Aufgabe von SCALANCE S623

Zusätzlich zu den Funktionen des SCALANCE S612 bietet der SCALANCE S623 mit einem zusätzlichen Port (DMZ) die Möglichkeit, ein zusätzliches Netzwerk anzubinden.

Mit dem SCALANCE S623 lässt sich am zusätzlichen Port eine DMZ (Demilitarisierte Zone) einrichten, in der Server platziert werden können, die sowohl aus dem unsicheren Netz (z. B. Internet oder externes Netz) als auch aus dem sicheren Netzwerk (internes Netz) erreicht werden müssen.

Der Port kann in Abhängigkeit vom Einsatzszenario verschiedene Funktionen erfüllen (nicht gleichzeitig):

- DMZ-Port
- Fernwartungsport

In typischen DMZ-Anwendungsfällen sollte der Anwender die Firewall-Regeln so projektieren, dass vom Internet (extern) Zugriffe auf die Server in der DMZ möglich sind (ggf. noch extra abgesichert durch einen VPN-Tunnel), nicht aber auf Geräte im gesicherten Bereich (intern).

1.8 Einsatz von CP 343-1 Advanced und CP 443-1 Advanced

Zellenschutzkonzept - Aufgabe von CP x43-1 Adv.

Mit Industrial Ethernet Security können einzelne Geräte, Automatisierungszellen oder Netzsegmente eines Ethernet-Netzwerks abgesichert werden. Zusätzlich kann die Datenübertragung durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall, NAT/NAPT-Router und VPN (Virtual Private Network) über IPsec-Tunnel geschützt werden vor:

- Datenspionage
- Datenmanipulation
- unberechtigten Zugriffen

Die Security-Funktionen vom CP x43-1 Adv. werden mit dem Projektierwerkzeug Security Configuration Tool konfiguriert, das in STEP 7 integriert ist.

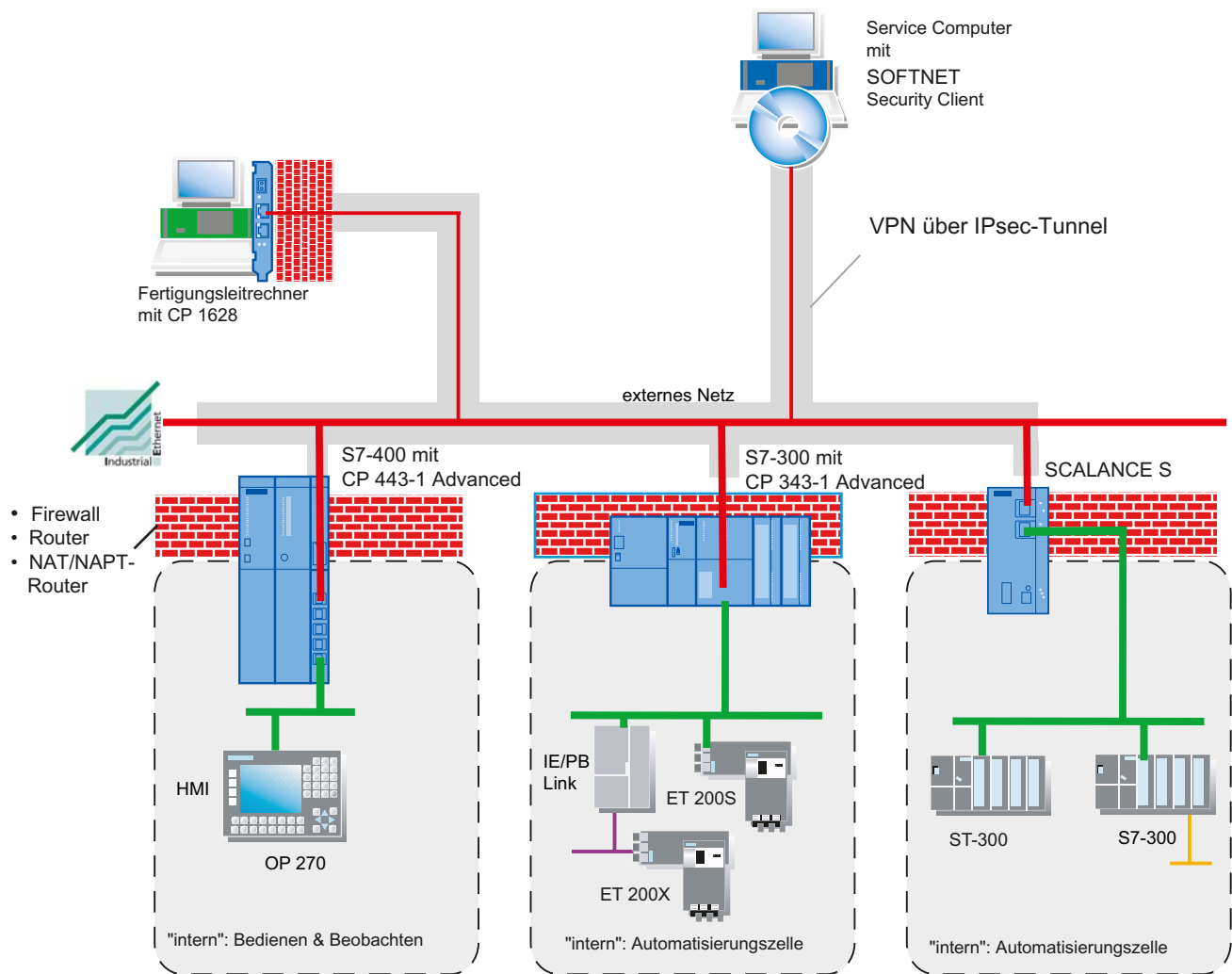


Bild 1-3 Netzkonfiguration mit CP x43-1 Adv.

Sicherheitsfunktionen

- Firewall
 - IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
 - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer 2)
 - Bandbreitenbegrenzung
 - Globale Firewall-Regeln

Alle Netzknoten, die sich im internen Netzsegment eines CP x43-1 Adv. befinden, werden durch dessen Firewall geschützt.

- Gesicherte Kommunikation durch IPsec-Tunnel

Der CP x43-1 Adv. kann mit anderen Security-Modulen per Projektierung zu Gruppen zusammengefasst werden. Zwischen allen Security-Modulen einer Gruppe werden IPsec-Tunnel aufgebaut (VPN). Alle internen Knoten dieser Security-Module können mittels dieser Tunnel gesichert miteinander kommunizieren.

- Logging

Zur Überwachung lassen sich Ereignisse in Log-Dateien speichern, die mit Hilfe des Projektierwerkzeugs ausgelesen werden oder automatisch an einen Syslog-Server gesendet werden können.

- HTTPS

Zur verschlüsselten Übertragung von Webseiten, z. B. bei der Prozesskontrolle.

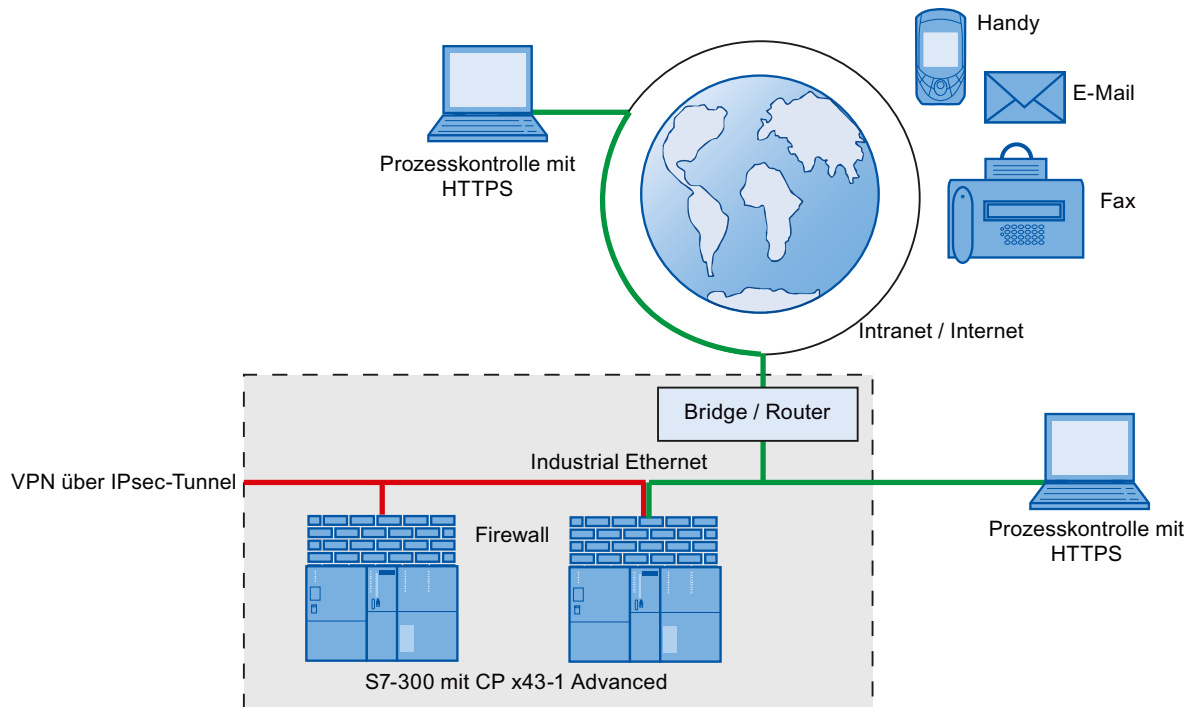


Bild 1-4 Prozesskontrolle mit HTTPS

- FTPS (expliziter Modus)
Zur verschlüsselten Übertragung von Dateien.
- Gesichertes NTP
Zur sicheren Uhrzeitsynchronisierung und -übertragung.
- SNMPv3
Zur abhörsicheren Übertragung von Netzwerkanalyseinformationen.
- Schutz für Geräte und Netzsegmente
Die Schutzfunktion Firewall und VPN kann sich über den Betrieb einzelner Geräte, mehrerer Geräte wie auch ganzer Netzsegmente erstrecken.

Interne und Externe Netzknoten :

CP x43-1 Adv. teilt Netzwerke in zwei Bereiche auf:

- internes Netz: geschützte Bereiche mit den "internen Knoten"
Interne Knoten sind alle diejenigen Knoten, die von einem CP x43-1 Adv. abgesichert sind.
- externes Netz: ungeschützte Bereiche mit den "externen Knoten"
Externe Knoten sind alle Knoten, die sich außerhalb der geschützten Bereiche befinden.

ACHTUNG
Die internen Netze werden als sicher (vertrauenswürdig) betrachtet. Verbinden Sie ein internes Netzsegment nur über CP x43-1 Adv. mit den externen Netzsegmenten. Weitere Verbindungswege zwischen dem internen und externen Netz dürfen nicht vorhanden sein.

Informationen zu allgemeinen Funktionen des CP x43-1 Adv.

In dem vorliegenden Handbuch erhalten Sie Informationen zu den Security-Funktionen des CP x43-1 Adv. Für Beschreibungen zu allgemeinen Funktionen siehe /1/ (Seite 217) bzw. /2/ (Seite 218).

1.9 Einsatz von CP 1628

Zellenschutzkonzept - Aufgabe von CP 1628

Die integrierten Sicherheitsmechanismen des CP 1628 ermöglichen die Absicherung von Rechnersystemen einschließlich der dazugehörigen Datenkommunikation innerhalb eines Automatisierungsnetzes oder den sicheren Fernzugriff über das Internet. Der CP 1628 erlaubt den Zugriff auf einzelne Geräte oder auch ganze Automatisierungszellen, die durch Security-Module geschützt sind und ermöglicht gesicherte Verbindungen über unsichere Netzwerkstrukturen.

Durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall und VPN (Virtual Private Network) über IPsec-Tunnel schützt der CP 1628 vor:

- Datenspionage
- Datenmanipulation
- unberechtigten Zugriffen

Die Security-Funktionen vom CP 1628 werden mit dem Projektierwerkzeug Security Configuration Tool konfiguriert, das in STEP 7 integriert ist.

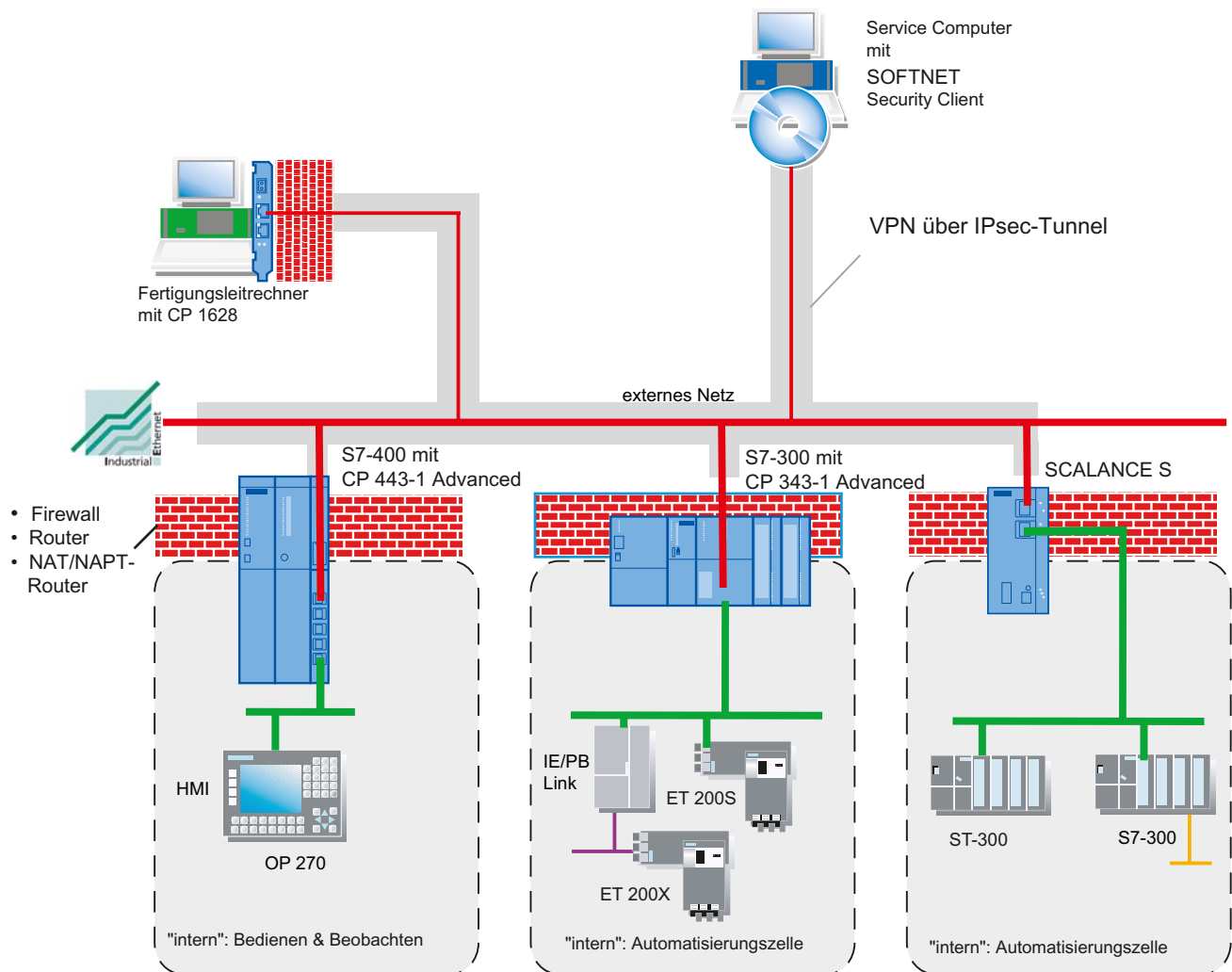


Bild 1-5 Netzkonfiguration mit CP 1628

Sicherheitsfunktionen

- Firewall
 - IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
 - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer 2)
 - Bandbreitenbegrenzung
 - Globale Firewall-Regeln
- Gesicherte Kommunikation durch IPsec-Tunnel

Der CP 1628 kann mit anderen Security-Modulen per Projektierung zu Gruppen zusammengefasst werden. Zwischen allen Security-Modulen einer Gruppe werden IPsec-Tunnel aufgebaut (VPN, Virtual Private Network).

Hinweis

Beachten Sie die Reihenfolge beim Laden auf die Baugruppen, wenn Sie die Firewall konfigurieren oder VPN-Einstellungen vornehmen.

Laden Sie zunächst alle VPN-Partner und zuletzt den CP 1628.

- Logging

Zur Überwachung lassen sich Ereignisse in Log-Dateien speichern, die mit Hilfe des Projektierwerkzeugs ausgelesen werden oder automatisch an einen Syslog-Server gesendet werden können.
- Gesichertes NTP

Zur sicheren Uhrzeitsynchronisierung und -übertragung.
- SNMPv3

Zur abhörsicheren Übertragung von Netzwerkanalyseinformationen.

Informationen zu allgemeinen Funktionen des CP 1628

In dem vorliegenden Handbuch erhalten Sie Informationen zu den Security-Funktionen des CP 1628 erklärt. Für Beschreibungen zu allgemeinen Funktionen siehe /11/ (Seite 221).

1.10 Projektierung und Administration

Das Wichtigste zusammengefasst

Im Zusammenspiel mit dem Projektierwerkzeug Security Configuration Tool werden Sie zu einer einfachen und sicheren Anwendung der Security-Module geführt:

- Projektierung ohne IT-Experten-Wissen mit dem Security Configuration Tool

Mit dem Security Configuration Tool können auch Nicht-IT-Experten ein Security-Modul projektieren. In einem erweiterten Modus können bei Bedarf komplexere Einstellungen vorgenommen werden.

- Gesicherte administrative Kommunikation

Die Übertragung der Einstellungen ist signiert und verschlüsselt und darf nur von autorisierten Personen durchgeführt werden.

- Zugriffsschutz im Security Configuration Tool

Durch die Benutzerverwaltung des Security Configuration Tool ist ein Zugriffsschutz für die Security-Module und die Projektierdaten gewährleistet.

- Wechselmedium C-PLUG einsetzbar

Der C-PLUG ist ein steckbares Wechselmedium, auf dem Konfigurationsdaten verschlüsselt abgespeichert sind. Er ermöglicht beim Austausch eines Security-Moduls die Konfiguration ohne PG/PC, sofern das Security-Modul eine Datenhaltung auf dem C-PLUG unterstützt. 

Projektierung mit Security Configuration Tool

Das Security Configuration Tool ist das zu den Security-Modulen mitgelieferte Projektierwerkzeug.

Das vorliegende Kapitel macht Sie mit der Bedienoberfläche und der Funktionsweise des Projektierwerkzeuges vertraut.

Sie erfahren, wie Security-Projekte eingerichtet, bedient und verwaltet werden.

Weitere Informationen

Wie Sie Module und IPsec-Tunnel konfigurieren, wird ausführlich in den Folgekapiteln dieses Handbuches erläutert.



Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe. Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

2.1 Funktionsumfang und Arbeitsweise

Leistungsumfang

Sie verwenden das Projektierwerkzeug Security Configuration Tool für diese Aufgaben:

- Projektierung der Security-Module
- Projektierung von SOFTNET Security Client
- Erstellen von Konfigurationsdaten für SCALANCE M
- Test- und Diagnosefunktionen, Statusanzeigen

Zwei Modi vom Security Configuration Tool

Das Security Configuration Tool gibt es in folgenden Modi:

- Security Configuration Tool Standalone: Kann unabhängig von STEP 7 aufgerufen werden. Keine Security-Projektierung von CPs möglich.
- Security Configuration Tool in STEP 7 integriert: Security-Projektierung von CPs sowie der Funktionsumfang von Standard Security Configuration Tool. Kann nur aus der STEP 7 Oberfläche heraus aufgerufen werden.

Betriebsarten

Das Security Configuration Tool verfügt über zwei Betriebsarten:

- Offline Projektierungssicht

In der Betriebsart Offline erfolgt die Projektierung der Konfigurationsdaten für die Security-Module und den SOFTNET Security Client. Vor dem Ladevorgang muss hierbei keine Verbindung zu dem Security-Modul bestehen.

- Online

Der Online-Modus dient dem Test und der Diagnose eines Security-Moduls.

Zwei Bedienungssichten

In der Betriebsart Offline stellt das Security Configuration Tool zwei Bedienungssichten zur Verfügung:

- Standard Modus

Der Standard Modus ist im Security Configuration Tool voreingestellt. Dieser Modus ermöglicht eine zügige, unkomplizierte Projektierung für den Betrieb der Security-Module.

- Erweiterter Modus

Im Erweiterten Modus gibt es erweiterte Einstellmöglichkeiten, die eine individuelle Einstellung der Firewall-Regeln und der Sicherheitsfunktionalität zulassen.

Arbeitsweise - Sicherheit und Konsistenz

- Zugriff nur für autorisierte Benutzer

Jedes Projekt ist durch Benutzername- und Passwortvergabe vor unberechtigttem Zugriff geschützt.

- Konsistente Projektdaten

Schon während der Eingabe in den einzelnen Dialogen erfolgen Konsistenzprüfungen. Zusätzlich können Sie jederzeit eine dialogübergreifende projektweite Konsistenzprüfung durchführen.

Auf die Security-Module können nur konsistente Projektdaten geladen werden.

- Schutz der Projektdaten durch Verschlüsselung

Die Projekt- und Konfigurationsdaten sind sowohl in der Projektdatei als auch auf dem C-PLUG (nicht für CP 1628) durch Verschlüsselung geschützt.

2.2 Installation

2.2.1 Unterstützte Betriebssysteme

Unterstützt Betriebssysteme

Unterstützt werden die folgenden Betriebssysteme:

- Microsoft Windows XP 32 Bit + Service Pack 3 
- Microsoft Windows 7 Professional 32/64 Bit oder
- Microsoft Windows 7 Professional 32/64 Bit + Service Pack 1
- Microsoft Windows 7 Ultimate 32/64 Bit
- Microsoft Windows 7 Ultimate 32/64 Bit + Service Pack 1
- Windows Server 2008 R2 64 Bit
- Windows Server 2008 R2 64 Bit + Service Pack 1
- PG/PC mit mindestens 128 MByte RAM-Speicher und einer CPU mit einer Taktfrequenz von mindestens 1 GHz.

ACHTUNG

Vor der Installation des Security Configuration Tool lesen Sie unbedingt die auf der CD mitgelieferte Datei "LIESMICH". In dieser Datei sind ggf. wichtige Hinweise und die letzten Änderungen vermerkt.

SCALANCE S und CP x34-1 Adv. - Gehen Sie so vor

Sie installieren das Projektierwerkzeug Security Configuration Tool von der mitgelieferten Produkt-CD.

- Legen Sie die Produkt-CD in Ihr CD-ROM-Laufwerk; bei eingeschalteter Autorun-Funktion wird die Oberfläche automatisch gestartet, von der aus Sie die Installation durchführen können.

oder

- Starten Sie die auf der mitgelieferten Produkt-CD vorhandene Anwendung "start.exe".

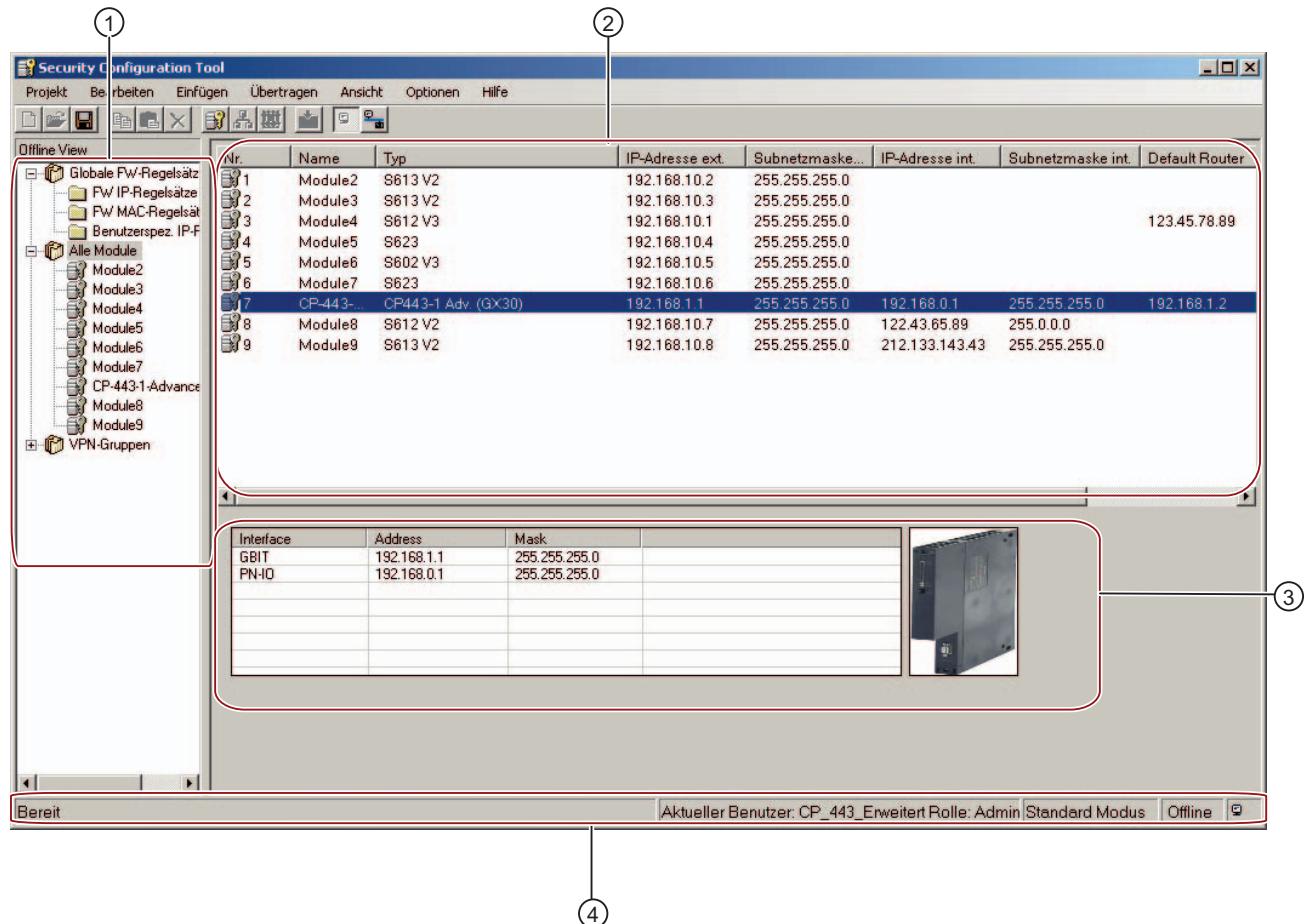
CP 1628 - Gehen Sie so vor

Sie installieren das Projektierwerkzeug Security Configuration Tool von der DVD "SIMATIC NET PC Software".

1. Starten Sie im Ordner "sw > Driverdisk > CP1628 > SCT" die Anwendung "setup.exe".
2. Klicken Sie durch das Setup und wählen Sie im Fenster "Programme" > "Selektion der zu installierenden Programme" das Programm "Security Configuration Tool V3.0".

2.3 Bedienoberfläche und Menübefehle

Aufbau der Bedienoberfläche im Erweiterten Modus



① Der Navigationsbereich fungiert als Projekt-Explorer mit den folgenden Hauptordnern:

- Globale FW-Regelsätze

Das Objekt enthält die projektierten globalen Firewall-Regelsätze. Weitere Ordner unterscheiden nach:

- IP-Regelsätze
- MAC-Regelsätze

- Benutzerspezifische IP-Regelsätze S≥V3.0

- Alle Module

Das Objekt enthält alle projektierten Security-Module bzw. SOFTNET Security Clients des Projekts.

- VPN-Gruppen

Das Objekt enthält alle erzeugten VPNs.

- ② Inhaltsbereich:
Indem Sie ein Objekt im Navigationsbereich anwählen, erhalten Sie im Inhaltsbereich Detailinformationen zu diesem Objekt.
Für SCALANCE S können die Adressdetails projiziert werden. Für SCALANCE M können Sie nur die IP-Adressen und die Subnetzmasken projektieren.
Durch Doppelklick auf die Objekte werden Eigenschaftsdialoge zur Eingabe weiterer Parameter geöffnet (nicht für SOFTNET Security Client und SCALANCE M).
- ③ Detail-Fenster:
Zusätzliche Details zum ausgewählten Objekt werden im Detail-Fenster angezeigt. Das Detail-Fenster kann aus- und eingeblendet werden.
- ④ Statuszeile:
Die Statuszeile zeigt Bedienzustände und aktuelle Statusmeldungen an. Hierzu gehören:
- Der aktuelle Benutzer und der Benutzertyp
 - Die Bedienungssicht - Standard Modus / Erweiterter Modus
 - Die Betriebsart - Online / Offline

Symbolleiste

Nachfolgend eine Übersicht der wählbaren Symbole in der Symbolleiste und deren Bedeutung.

Symbol	Bedeutung / Bemerkungen
	Neues Projekt anlegen.
	Bestehendes Projekt öffnen.
	Geöffnetes Projekt unter aktuellem Pfad und Projektnamen speichern.
	Angewähltes Objekt kopieren.
	Objekt aus der Zwischenablage einfügen.
	Angewähltes Objekt löschen.
	Neues Modul anlegen. Das Symbol ist nur aktiv, wenn Sie sich innerhalb des Navigationsbereiches im Ordner "Alle Module" oder auf einer VPN-Gruppe befinden.
	Neue Gruppe anlegen. Das Symbol ist nur aktiv, wenn Sie sich innerhalb des Navigationsbereiches im Ordner "VPN-Gruppen" befinden.

Symbol	Bedeutung / Bemerkungen
	Einen neuen global gültigen oder benutzerspezifischen IP-Regelsatz oder einen globalen MAC-Regelsatz anlegen. Das Symbol ist nur aktiv, wenn Sie sich innerhalb des Navigationsbereiches in einem Unterordner von "Globale FW-Regelsätze" oder auf dem Ordner "Benutzerspez. IP-Regelsätze" befinden.
	 Konfiguration in die selektierten Security-Module laden bzw. Konfigurationsdaten für SOFTNET Security Client / SCALANCE M erstellen.
	In den Offline-Modus umschalten.
	In den Online-Modus umschalten.

Menüleiste

Nachfolgend eine Übersicht der wählbaren Menübefehle und deren Bedeutung.

Menübefehl		Bedeutung / Bemerkungen	Tastenkombination
Projekt ▶...		Funktionen für die projektspezifischen Einstellungen sowie das Laden und Speichern der Projektdatei.	
	Neu...	Neues Projekt anlegen. Für CP: Projekte werden durch STEP 7-Projektierung angelegt.	
	Öffnen...	Bestehendes Projekt öffnen. Für CP: Bestehende Projekte können nur über STEP 7-Projekte geöffnet werden.	
	Speichern...	Geöffnetes Projekt unter aktuellem Pfad und Projektnamen speichern.	
	Speichern unter...	Geöffnetes Projekt unter wählbarem Pfad und Projektnamen speichern. Für CP: Das Projekt ist Teil vom STEP 7-Projekt. Der Pfad kann nicht geändert werden.	
	Eigenschaften...	Dialog für Projekteigenschaften öffnen.	
	Zuletzt geöffnete Projekte	Direkte Auswahlmöglichkeit der bisher bearbeiteten Projekte. Für CP: Bestehende Projekte können nur über STEP 7-Projekte geöffnet werden.	
	Beenden	Projekt schließen.	
Bearbeiten ▶...		Menübefehle nur im Offline-Modus Hinweis Die Funktionen können Sie bei angewähltem Objekt teilweise auch über das Kontextmenü auswählen.	
	Kopieren	Angewähltes Objekt kopieren.	Strg + C

Menübefehl		Bedeutung / Bemerkungen	Tastenkombination
	Einfügen	Objekt aus der Zwischenablage holen und einfügen.	Strg + V
	Löschen	Angewähltes Objekt löschen.	Entf
	Umbenennen	Angewähltes Objekt umbenennen.	F2
	Modul austauschen...	Angewähltes Security-Modul durch ein anderes austauschen.	
	Eigenschaften...	Eigenschaftsdialog des angewählten Objektes öffnen.	F4
	Online-Diagnose...	Auf die Test- und Diagnosefunktionen zugreifen. Der Menübefehl ist nur in der Online-Ansicht sichtbar.	
Einfügen ▶...		Menübefehle nur im Offline-Modus	
	Modul	Neues Modul anlegen. Der Menübefehl ist nur aktiv, wenn ein Modul oder eine Gruppe im Navigationsbereich angewählt ist.	Strg + M
	Gruppe	Neue Gruppe anlegen. Der Menübefehl ist nur aktiv, wenn ein Gruppen-Objekt im Navigationsbereich angewählt ist.	Strg + G
	Firewall-Regelsatz	Einen neuen global gültigen Firewall IP-Regelsatz oder MAC-Regelsatz anlegen. Der Menübefehl ist nur aktiv, wenn ein Firewall-Objekt im Navigationsbereich angewählt ist.	Strg + F
Übertragen ▶...			
	An Modul(e)...	Konfiguration in das selektierte Security-Modul laden bzw. Konfigurationsdaten für SOFTNET Security Client / SCALANCE M erstellen. Anmerkung: Es können nur konsistente Projektdaten geladen werden. Für CPs: Projektdaten können nur über STEP 7 geladen werden.	
	An alle Module...	Konfiguration in alle Security-Module laden. Anmerkung: Es können nur konsistente Projektdaten geladen werden.	
	Konfigurationszustand...	Konfigurationszustand der projektierten Security-Module wird in einer Liste angezeigt.	
	Firmware übertragen...	Neue Firmware in selektiertes Security-Modul laden. Für S7-CPs: Die Firmware wird über das Aktualisierungs-Zentrum der Web-Diagnose auf den CP geladen.	
Ansicht ▶...			

Menübefehl		Bedeutung / Bemerkungen	Tastenkombination
	Erweiterter Modus	Vom Standard Modus (Voreinstellung) in den Erweiterten Modus umschalten. Achtung Sie können eine einmal vorgenommene Umschaltung in den Erweiterten Modus für das aktuelle Projekt nur rückgängig machen, wenn Sie keine Änderungen vorgenommen haben.	Strg + E
	Detail-Fenster ausblenden	Zusätzliche Details zum ausgewählten Objekt aus- und einblenden.	Strg + Alt + D
	Offline	Ist Voreinstellung. Umschaltung in die Projektierungsbetriebsart.	Strg + Shift + D
	Online	Umschaltung in die Test- und Diagnosebetriebsart.	Strg + D
Optionen ▶...			
	IP-Dienste...	Dialog für Dienst-Definitionen für IP-Firewall-Regeln öffnen. Der Menübefehl ist nur im Erweiterten Modus sichtbar.	
	MAC-Dienste...	Dialog für Dienst-Definitionen für MAC-Firewall-Regeln öffnen. Der Menübefehl ist nur im Erweiterten Modus sichtbar.	
	Netzwerkadapter...	Über den ausgewählten Netzwerkadapter wird dem SCALANCE S eine IP-Adresse zugewiesen.	
	Sprachen...	Sprache auswählen, in der die SCT-Oberfläche angezeigt wird. Für SCT in STEP 7 wird die Sprache der SCT-Oberfläche über die Sprachauswahl in STEP 7 festgelegt.	
	Log-Dateien...	Anzeige von gespeicherten Log-Dateien.	
	Symbolische Namen...	Symbolische Namen für IP- oder MAC-Adressen vergeben.	
	NTP-Server...	NTP-Server erstellen und bearbeiten.	
	Konsistenzprüfungen...	Konsistenz des gesamten Projektes prüfen. Als Ergebnis wird eine Resultatsliste ausgegeben.	
	Benutzerverwaltung...	Benutzer und Rollen anlegen und bearbeiten sowie Rechte zuweisen.	
	Zertifikatsmanager...	Zertifikate anzeigen oder importieren / exportieren.	
Hilfe ▶...			
	Inhalt...	Hilfe zu den Funktionen und Parametern, die Sie im SCT vorfinden.	Strg + Shift + F1
	Index...	Hilfe zu den Funktionen und Parametern, die Sie im SCT vorfinden.	Strg + Shift + F2
	Info...	Informationen zum Versions- und Ausgabestand des SCT.	

2.4 Projekte anlegen und verwalten

2.4.1 Security Configuration Tool Standalone



Projektierung mit dem Security Configuration Tool Standalone

Das Security Configuration Tool Standalone wird für die Erstellung von Security-Projekten verwendet, in welchen keine Security-Module projiziert werden, die in STEP 7 erstellt und konfiguriert werden müssen.

Über den Menübefehl "Projekt" > "Neu..." legen Sie ein neues Projekt an. Dieses umfasst sämtliche Konfigurations- und Verwaltungsinformationen für ein oder mehrere SCALANCE S, SOFTNET Security Clients sowie SCALANCE M-Geräte. Für jedes Gerät legen Sie im Projekt ein Modul an.

2.4.2 Security Configuration Tool in STEP 7

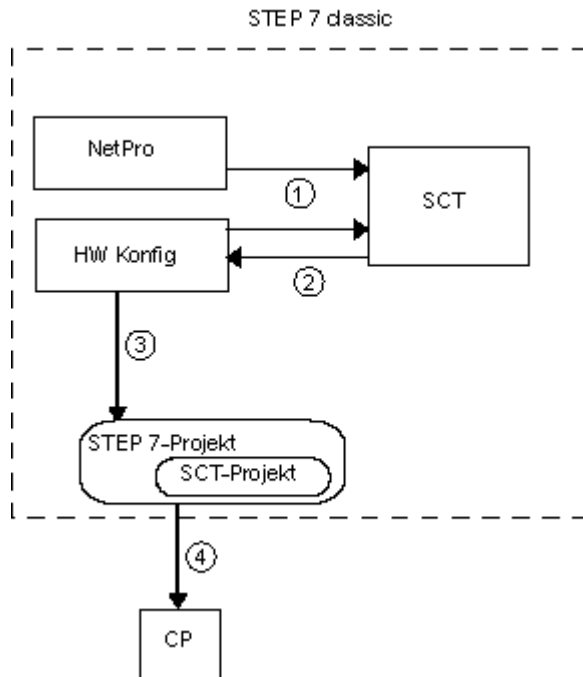
Projektierung

Das Security Configuration Tool in STEP 7 wird für die Erstellung von Security-Projekten verwendet, in welchen Security-Module projiziert werden, die in STEP 7 erstellt und konfiguriert werden müssen. Zusätzlich werden alle Security-Module der Standalone-Variante unterstützt.

Sobald Sie in STEP 7 für ein Security-Modul die Security-Funktion aktivieren, wird automatisch ein SCT-Projekt angelegt, in welchem die Daten der Security-Konfiguration abgelegt und verwaltet werden. Sämtliche Daten zur Security-Konfiguration werden intern von SCT bearbeitet und das Ergebnis an STEP 7 zurückgeliefert.

Zusammenspiel von STEP 7 und SCT

Das Zusammenspiel von STEP 7 und SCT wird anhand der folgenden Darstellung erläutert:



- ① Nehmen Sie über STEP 7 Security-Einstellungen vor, wird SCT aufgerufen, da dort die Daten für Security gepflegt und verwaltet werden.
Sind in NetPro spezifizierte Verbindungen projektiert, werden für diese nach dem Speichern und Übersetzen automatisch Firewall-Regeln in SCT angelegt.
- ② In SCT nehmen Sie weitere Security-Einstellungen vor. SCT bearbeitet die Daten intern und gibt das Ergebnis an STEP 7 zurück.
- ③ Aktionen wie "Speichern Unter" und "Übersetzen" finden innerhalb von STEP 7 statt. Die Security-Daten werden als SCT-Projekt unter einem automatisch vergebenen Namen in einem Unterordner des STEP 7-Projektes gespeichert. Name und Speicherort dürfen nicht verändert werden. Für ein STEP 7-Projekt kann genau ein SCT-Projekt angelegt werden. Ein mit dem Security Configuration Tool in STEP 7 angelegtes SCT-Projekt kann nicht mit dem Security Configuration Tool im Standalone-Modus geöffnet werden.
- ④ Die projektierten Security-Daten des CP werden über STEP 7 auf die Baugruppe geladen.

Welche Daten werden von STEP 7 nach SCT migriert und im Inhaltsbereich angezeigt?

Folgende in STEP 7 angelegten Projektierungsdaten werden automatisch von SCT übernommen, können dort jedoch nicht verändert werden:

- Geräte name
- IP-Adresse intern
- IP-Adresse extern

- Subnetzmaske intern
- Subnetzmaske extern
- MAC-Adresse
- Standard-Router

Welche Daten können nach SCT migriert und dort verändert werden?

Nach SCT migriert und dort verändert werden können bereits in STEP 7 angelegt:

- Access Control-Listen 
- Benutzer
- NTP-Server



Detailinformationen dazu finden Sie in der Online-Hilfe von SCT.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen SCT-Dialog.

Automatische Firewall-Regeln für spezifizierte Verbindungen

Für in STEP 7 projektierte spezifizierte Verbindungen werden automatisch Firewall-Regeln in SCT angelegt, die den Verbindungsaufbau freigeben. Nähere Information hierzu finden Sie im Kapitel Verbindungsbezogene automatische Firewall-Regeln (Seite 112).

Für unspezifizierte Verbindungen müssen Sie die Firewall-Regeln, die den Verbindungsaufbau freigeben, in SCT konfigurieren. Nähere Information hierzu finden Sie im Kapitel Im Erweiterten Modus (Seite 106).

Security-Einstellungen in STEP 7 vornehmen

Security-Einstellungen nehmen Sie alternativ wie folgt vor:

- Über einzelne Register der Objekteigenschaften

In einzelnen Registern können Sie CP-spezifische Security-Funktionen aktivieren und ausführen. Beim Ausführen wird der entsprechende SCT-Dialog geöffnet, in dem Sie Security-Einstellungen vornehmen können. In folgenden Register können Sie Security-Einstellungen vornehmen:

	Register	Funktion	Beschreibung
	Security	Security aktivieren	- Die Security-Funktionen in den einzelnen Registern werden aktiv. - Das Menü "Bearbeiten" > "Security Configuration Tool" wird aktiv, über welches Sie das Security Configuration Tool öffnen. Dort können Sie weitere, Security-Modul übergreifende Einstellungen vornehmen, wie z. B. VPN-Gruppen anlegen oder Security-Module hinzufügen, die nicht in STEP 7 projektierbar sind. - Falls Sie für das Security-Modul Benutzer in STEP 7 projektiert haben, öffnet sich das Fenster "Datenmigration für securityrelevante Projektdaten", über das Sie die Benutzer in das Security Configuration Tool migrieren können.
		Start der Security-Konfiguration	SCT öffnet sich in einem Übersichtsmodus, in dem Sie die für dieses Security-Modul spezifischen Eigenschaften konfigurieren können.
		Firewall-Regeln nachladen	Angepasste Firewall-Einstellungen werden generiert und auf den CP geladen, ohne ein Stoppen des CP zu verursachen.
		Firewall-Regeln online nachladen (CP 1628)	Angepasste Firewall-Einstellungen werden generiert und online auf den CP geladen.
	Benutzer	Start der Benutzerverwaltung	Startet die SCT-Benutzerverwaltung, in der Benutzer und Rollen angelegt sowie Rechte zugewiesen werden.
	IP-Zugriffsschutz	Start der Firewall-Konfiguration	Beim Aktivieren von Security wird eine vorhandene IP-Zugriffsliste über eine Umsetzung in Firewall-Regeln in das Security Configuration Tool migriert.
	FTP	Zugriff nur über FTPS zulassen	Startet die SCT-Benutzerverwaltung, in der Sie einer Rolle FTP-Rechte zuweisen können.
		Start der Benutzerverwaltung	
	Web	Zugriff nur über HTTPS zulassen	Startet die SCT-Benutzerverwaltung, in der Sie einer Rolle Web-Rechte zuweisen können.
		Start der Benutzerverwaltung	
	Uhrzeitsynchronisation	Erweiterte NTP-Konfiguration	Startet das SCT im NTP-Konfigurationsmodus.
	SNMP	Start der SNMP-Konfiguration	Startet SCT im SNMP-Konfigurationsmodus. Sie können zwischen SNMPv1 oder SNMPv3 wählen.
		Start der Benutzerverwaltung	Startet die SCT-Benutzerverwaltung, in der Sie einer Rolle SNMP-Rechte zuweisen können.

- Direkt in SCT

Sie rufen SCT in STEP 7 über das Menü "Bearbeiten" > "Security Configuration Tool" auf. Zusätzlich zu den Einstellungen in den Registern der Objekteigenschaften legen Sie hier z. B. VPN-Gruppen an oder fügen SCALANCE S-Module hinzu. Die SCALANCE S-Module können Sie in SCT zwar projektieren und laden, die Daten werden jedoch nicht an STEP 7 zurückgeliefert. Auch werden die Module nach Beendigung vom SCT nicht in STEP 7 angezeigt.

Hinweis

Nähere Angaben finden Sie in der STEP 7 und in der SCT Online-Hilfe.

Allgemeine Informationen zu STEP 7 finden Sie in /9/ (Seite 220).

2.4.3 STEP 7-Daten migrieren

Sicherheitsrelevante Projektdaten migrieren

S7-CP

Bei der Aktivierung von Security werden die folgenden in STEP 7 vorgenommenen Einstellungen automatisch in einen sicheren Anwendungsbereich migriert:

- NTP-Server - siehe Kapitel Zeitsynchronisierung (Seite 153)
- IP Access Control-Listen - siehe Kapitel Zugriffsliste projektieren (Seite 93)

Nicht automatisch migriert werden Benutzer und deren Passwörter.

Firewall-Regeln für spezifizierte Verbindungen

Für in STEP 7 projektierte spezifizierte Verbindungen werden automatisch Firewall-Regeln in SCT angelegt, die den Verbindungsaufbau freigeben.

Für unspezifizierte Verbindungen müssen Sie die Firewall-Regeln, die den Verbindungsaufbau freigeben, in SCT konfigurieren.

STEP 7-Gerätebenutzer in die SCT-Benutzerverwaltung migrieren

Wählen Sie in dem Migrationsdialog aus, wie die in STEP 7 angelegten Benutzer in die SCT-Benutzerverwaltung migriert werden sollen. Dabei stehen Ihnen folgende Aktionen zur Auswahl:

Aktion	Beschreibung
Übernehmen als...	Der Benutzer wird unter einem anderen Namen in die SCT-Benutzerverwaltung migriert. Geben Sie den Namen in die Spalte "Migrierter Benutzername" ein. Dem migrierten Benutzer wird in SCT eine automatisch generierte Rolle zugewiesen.
Zusammenführen	Ist im SCT-Projekt bereits ein Benutzer mit dem gleichen Namen angelegt, werden die beiden Benutzer zusammengelegt. Die Rolle dieses Benutzers wird um die ausgewählten Rechte des migrierten Benutzers erweitert.
Nicht übernehmen	Der Benutzer des Security-Moduls wird nicht in die SCT-Benutzerverwaltung migriert. Eine nachträgliche Migration ist nicht möglich.

Hinweis

Folgende Daten werden nicht migriert

- Passwörter bereits angelegter Benutzer in STEP 7. Wählen Sie deshalb für jeden Benutzer aus, wie er migriert werden soll und vergeben Sie über die Schaltfläche "Passwort vergeben" ein neues Passwort.
- Der in STEP 7 verfügbare systemdefinierte Benutzer "everybody". Auch werden dessen Rechte für migrierte Benutzer nicht übernommen.

STEP 7-Gerätrechte in die SCT-Benutzerverwaltung migrieren

Folgende Rechte werden migriert:

Recht in STEP 7	Recht nach der Migration in SCT	Service
Auf die projektierten Symbole zuzugreifen	Applet: Variablen über projektierte Symbole lesen	SPS
	Applet: Variablen über projektierte Symbole schreiben	
Variablen über absolute Adressen zu lesen	Applet: Variablen über absolute Adressen lesen	
Variablen über absolute Adresse zu schreiben	Applet: Variablen über absolute Adressen schreiben	
Mit FTP auf Dateien in der S7-Station zugreifen	FTP: Dateien (DBs) von der S7-CPU lesen	Dateisystem
	FTP: Dateien (DBs) in die S7-CPU schreiben	
	FTP: Dateien vom CP-Dateisystem lesen	
	FTP: Dateien auf das CP-Dateisystem schreiben	

Recht in STEP 7	Recht nach der Migration in SCT	Service
	Web: CP-Dateisystem formatieren	
Eine Testmail über die Systemseite zu versenden	Web: Auf Web-Diagnose und CP-Dateisystem zugreifen	Web
	Web: Testmail versenden	
Den Status von Baugruppen abzufragen	Applet: Status der Baugruppen im Rack lesen	SPS
Die Bestellnummer von Baugruppen abzufragen	Applet: Bestellnummer der Baugruppen im Rack lesen	

2.4.4 Übersicht

Allgemeine Inhalte

In beiden SCT-Versionen werden Sie beim Anlegen eines neuen Projektes aufgefordert, einen Benutzernamen und ein Passwort zu vergeben. Der Benutzer, den Sie hier anlegen, ist vom Typ "administrator". Nach der Eingabe können Sie die Einstellungen im Projekt vornehmen.

Allgemein beinhalten die Konfigurationen eines Projektes:

- Projektweit gültige Einstellungen
- Modulspezifische Einstellungen
- Gruppenzuordnungen für IPsec-Tunnel 

Zusätzlich regelt eine Benutzerverwaltung die Zugriffsberechtigungen auf die Projektdaten und damit auf die Security-Module.

Projektweit gültige Einstellungen

- Projekteigenschaften
Diese umfassen neben allgemeinen Adress- und Namensangaben Vorgaben für Initialisierungswerte.
- Globale Firewall-Regelsätze
Globale Firewall-Regeln können mehreren Modulen gleichzeitig zugewiesen werden. Diese Möglichkeit vereinfacht in vielen Fällen die Projektierung im Gegensatz zur Projektierung von lokalen Firewall-Regelsätzen in den modulspezifischen Einstellungen.
- Dienst-Definitionen
Mit Hilfe der Definition von IP- oder MAC-Diensten können Sie Firewall-Regeln kompakt und übersichtlich definieren.
- NTP-Server
NTP-Server werden projektweit angelegt und können dann in SCT mehreren Security-Modulen zugewiesen werden.

- **Zertifikatsverwaltung**
In der Zertifikatsverwaltung werden sämtliche Zertifikate des Projektes verwaltet.
- **Benutzerverwaltung**
In der Benutzerverwaltung können Sie alle Benutzer des Projektes und deren Rechte verwalten.
- **Symbolische Namen**
In einem Projekt können Sie stellvertretend für IP- und MAC-Adressen symbolische Namen in einer Tabelle vergeben

Modulspezifische Einstellungen

Die meisten Funktionen werden im Eigenschaftsdialog eines Moduls konfiguriert. Hier eine Übersicht der angebotenen Register und deren Funktion:

	Funktion / Register im Eigenschaftsdialog	wird angeboten im Modus	
		Standard	Erweiterter
	Schnittstellen Übersicht der einzelnen Porteeinstellungen. Für CPs: Die Einstellungen werden aus STEP 7 übernommen und können nicht verändert werden. Für SCALANCE S ≥ V3.0: Zusätzlich können Einstellungen zum DMZ-Port, Aktivierung von DynDNS und PPPoE usw. vorgenommen werden.	X	X
	Routing Geben Sie hier die Daten zum Standard-Router ein und/oder legen Sie eine Route fest. Für CPs: Die Angabe eines Standard-Routers wird aus STEP 7 übernommen und kann auch nur dort verändert werden. Die Anzeige erfolgt im Inhaltsbereich von SCT. Das Register ist in den Moduleigenschaften daher nicht vorhanden.	X	X
	Firewall Im Standard Modus aktivieren Sie hier die Firewall mit einfachen Standard-Regeln. Zusätzlich können Sie Log-Einstellungen aktivieren. Im Erweiterten Modus können Sie detaillierte Paketfilter-Regeln definieren. Außerdem können Sie für jede Paketfilter-Regel explizite Log-Einstellungen definieren. Für CPs: Falls eine Access Control-Liste migriert wurde, wird diese hier angezeigt und kann bearbeiten werden.	X	X
	Zeitsynchronisierung Legen Sie hier die Synchronisationsart für Datum und Uhrzeit fest.	X	X
	Log-Einstellungen Sie können hier genauere Angaben zum Aufzeichnungs- und Speichermodus von Log-Ereignissen treffen und die Übertragung zu einem Syslog-Server projektieren.	-	X

	Funktion / Register im Eigenschaftendialog	wird angeboten im Modus	
		Standard	Erweiterter
	Knoten Nehmen Sie je nach Security-Modul Einstellungen zu Subnetzen, IP/MAC-Knoten und NDIS-Knoten vor, welche zusätzlich über die VPN-Tunnel erreicht werden sollen. Für SCALANCE S: Das Lernen von internen Knoten kann aktiviert oder deaktiviert werden.	-	X
	VPN Befindet sich das Modul in einer Gruppe können Sie hier die Dead-Peer-Detection, die Art des Verbindungsaufbaus und ggf. eine WAN-IP-Adresse konfigurieren.	X	X
	NAT Aktivieren Sie NAT/NAPT-Router und legen Sie in einer Liste die Adressumsetzung fest.	-	X
	DHCP-Server Für das interne Netz können Sie das Modul als DHCP-Server aktivieren. Für SCALANCE S 623: Befindet sich der DMZ-Port im Betriebsmodus DMZ, kann für diesen Port auch ein DHCP-Server eingerichtet werden.	-	X
	SNMP Stellen Sie in diesem Register die SNMP-Protokollversion und das Authentifizierungs-/Verschlüsselungsverfahren ein.	-	X
	Proxy-ARP Statische Einträge für Proxy-ARP auf externer Schnittstelle vornehmen.	-	X

Die ausführliche Beschreibung dieser Funktionen finden Sie im Kapitel Weitere Moduleigenschaften projektieren (Seite 133).

Gruppenzuordnungen für IPsec-Tunnel



VPN-Gruppen legen fest, welche Security-Module, SOFTNET Security Clients und SCALANCE M-Module miteinander über IPsec-Tunnel kommunizieren sollen.

Indem Sie Security-Module, SOFTNET Security Clients und SCALANCE M-Module einer Gruppe zuordnen, können diese Module über ein VPN (Virtual Private Network) Kommunikationstunnel aufbauen.

Nur Module der gleichen Gruppe können untereinander gesichert über Tunnel kommunizieren, wobei Security-Module, SOFTNET Security Clients und SCALANCE M-Module mehreren Gruppen gleichzeitig angehören können.

2.4.5 Initialisierungswerte für ein Projekt festlegen



Initialisierungswerte für ein Projekt festlegen

Mit den Initialisierungswerten legen Sie Eigenschaften fest, die beim Anlegen neuer Module automatisch übernommen werden. Außerdem legen Sie fest, ob beim Anlegen eines neuen Security-Moduls ein Fenster zum Einstellen der Eigenschaften geöffnet werden soll oder ob das Security-Modul direkt eingefügt wird.

Wählen Sie den Menübefehl "Projekt" > "Eigenschaften...", Register "Standard-Initialisierungswerte".

Schutz der Projektdaten durch Verschlüsselung

Die abgespeicherten Projekt- und Konfigurationsdaten sind sowohl in der Projektdatei als auch auf dem C-PLUG (nicht für CP 1628) durch Verschlüsselung geschützt.

2.4.6 Konsistenzprüfungen

Übersicht

Security Configuration Tool unterscheidet:

- Lokale Konsistenzprüfungen
- Projektweite Konsistenzprüfungen

Auf welche geprüften Regeln Sie bei der Eingabe achten müssen, finden Sie in den jeweiligen Dialogbeschreibungen unter dem Stichwort "Konsistenzprüfung".

Lokale Konsistenzprüfungen

Eine Konsistenzprüfung heißt lokal, wenn sie direkt innerhalb eines Dialogs durchgeführt werden kann. Bei folgenden Aktionen können Prüfungen ablaufen:

- nach dem Verlassen eines Feldes
- nach dem Verlassen einer Zeile in einer Tabelle
- beim Verlassen des Dialogs mit "OK"

Projektweite Konsistenzprüfungen

Projektweite Konsistenzprüfungen geben Aufschluss über korrekt konfigurierte Module. Da während der Erstellung eines Projekts oft inkonsistente Projektdaten konfiguriert werden und eine ständige projektweite Konsistenzprüfung zu viel Zeit kostet, erfolgt nur bei folgenden Aktionen eine automatische Prüfung:

- beim Speichern des Projekts
- beim Öffnen des Projekts
- vor dem Laden einer Konfiguration

ACHTUNG
Projektiertaten können Sie nur laden, wenn das Projekt insgesamt konsistent ist.

So veranlassen Sie eine projektweite Konsistenzprüfung

Führen Sie die Konsistenzprüfung für ein geöffnetes Projekt folgendermaßen durch:

Menübefehl: "Optionen" > "Konsistenzprüfungen".

Das Prüfergebnis wird in einer Liste ausgegeben. Wenn das Projekt inkonsistente Daten enthält, wird der Status in der Statuszeile des SCT-Fensters angezeigt. Klicken Sie auf die Statuszeile, um die Prüfliste anzuzeigen.

2.4.7 Symbolische Namen für IP-/MAC-Adressen vergeben

So erreichen Sie diese Funktion

Menübefehl: "Optionen" > "Symbolische Namen...".

Bedeutung und Vorteil

In einem Security-Projekt können Sie stellvertretend für IP- und MAC-Adressen symbolische Namen in einer Tabelle vergeben.

Die Projektierung der einzelnen Dienste kann dadurch einfacher und sicherer erfolgen.

Bei den folgenden Funktionen und deren Projektierung werden symbolische Namen innerhalb des Projekts berücksichtigt:

- Firewall
- NAT/NAPT-Router
- Syslog
- DHCP

Gültigkeit und Eindeutigkeit

Die Gültigkeit der in der Tabelle angegebenen symbolischen Namen ist auf die Projektierung innerhalb eines Security-Projekts beschränkt.

Innerhalb des Projekts muss jeder symbolische Name eindeutig einer einzigen IP-Adresse oder MAC-Adresse zugeordnet werden.

Automatische Übernahme symbolischer Namen in die Symboltabelle von SCT

Sie können symbolische Namen in den genannten Funktionen anstelle von IP-Adressen verwenden, z. B. beim Anlegen von Firewall-Regeln, ohne dass diese in der hier beschriebenen Tabelle bereits vergeben sind.

So vergebene symbolische Namen werden automatisch in die Tabelle übernommen und können zu einem späteren Zeitpunkt noch zugeordnet werden. Im Rahmen der Konsistenzprüfung werden Sie auf fehlende Zuordnungen hingewiesen.

Dialog zum Vergeben symbolischer Namen

Um Inkonsistenzen zwischen einer Zuordnung "IP-Adresse - symbolischer Name" sowie "MAC-Adresse - symbolischer Name" zu vermeiden, werden die symbolischen Namen in einer einzigen Tabelle verwaltet.

Gehen Sie so vor, um neue Einträge in die Symboltabelle von SCT aufzunehmen:

1. Betätigen Sie die Schaltfläche "Hinzufügen", um einen neuen symbolischen Namen in der nächsten freien Tabellenzeile hinzuzufügen.
2. Geben Sie den symbolischen Namen DNS-konform ein. Siehe Abschnitt DNS-Konformität (Seite 215).
3. Ergänzen Sie den Eintrag mit der IP-Adresse oder der MAC-Adresse. Sie können auch beide Adressen angeben.

Symbolische Namen

Bitte geben Sie in jeder Zeile einen Namen für das Gerät sowie mindestens eine IP-Adresse oder eine MAC-Adresse ein. (Es können auch IP-Adresse und MAC-Adresse eingegeben werden.)

Name	IP-Adresse	MAC-Adresse
SPS1	192.168.56.2	
SPS2		00-0E-8C-01-23-45
SPS3	192.168.56.3	00-0E-8C-66-77-88
Test	192.168.10.1	
SPS4	192.168.56.4	
ZIP	192.168.56.5	
GlobIPquelle	192.168.56.6	
GlobIPziel	192.168.56.7	
QIP	192.168.56.8	

Hinzufügen Entfernen

OK Abbrechen Hilfe

Gehen Sie so vor, um automatische Einträge in die Tabelle aufzunehmen:

Wenn der symbolische Name im Rahmen der Definition eines Dienstes bereits angegeben wurde, finden Sie einen entsprechenden Eintrag in der Tabelle.

1. Klicken Sie in der entsprechenden Tabellenzeile in die Spalte für die IP-Adresse oder für die MAC-Adresse.
2. Ergänzen Sie den Eintrag mit der IP-Adresse oder der MAC-Adresse. Sie können auch beide Adressen angeben.

Falls Sie einen Eintrag in der Tabelle löschen, bleiben die in den Diensten verwendeten symbolischen Namen dort bestehen. Die Konsistenzprüfung erkennt in diesem Falle nicht definierte symbolische Namen. Dies gilt sowohl für manuell als auch für automatisch erzeugte Einträge.

**Tipp:**

Für die hier beschriebene Tabelle ist die Anwendung der projektweiten Konsistenzprüfung besonders sinnvoll. Sie können anhand der Liste Unstimmigkeiten erkennen und korrigieren.

Starten Sie die Konsistenzprüfung für ein geöffnetes Projekt über den Menübefehl "Optionen" > "Konsistenzprüfungen".

Konsistenzprüfung - diese Regeln müssen Sie beachten

Berücksichtigen Sie bei Ihrer Eingabe die nachfolgend aufgeführten Regeln.

Prüfung / Regel	Prüfung erfolgt ¹⁾	
	lokal	projektweit
Die Zuordnung eines symbolischen Namens zu einer IP- oder MAC-Adresse muss eindeutig sein. Der Symbolname und die Adresse dürfen nur einmal vergeben werden und nicht in einem anderen Listeneintrag verwendet werden.	x	
Die symbolischen Namen müssen DNS-konform sein.	x	
Einem symbolischen Namen muss entweder eine IP-Adresse oder eine MAC-Adresse oder beides zugeordnet sein.	x	
Den IP-Adressen der Security-Module dürfen keine symbolischen Namen zugewiesen sein.		x
Im Projekt für IP- oder MAC-Adressen verwendete symbolische Namen müssen in der Tabelle enthalten sein. Inkonsistenzen können dadurch entstehen, dass Einträge in der Tabelle gelöscht und in den Projektiertools nicht entsprechend entfernt oder korrigiert werden.		x

¹⁾ Beachten Sie die Erläuterungen im Kapitel Konsistenzprüfungen (Seite 52).

2.5 Konfigurationsdaten für SCALANCE M

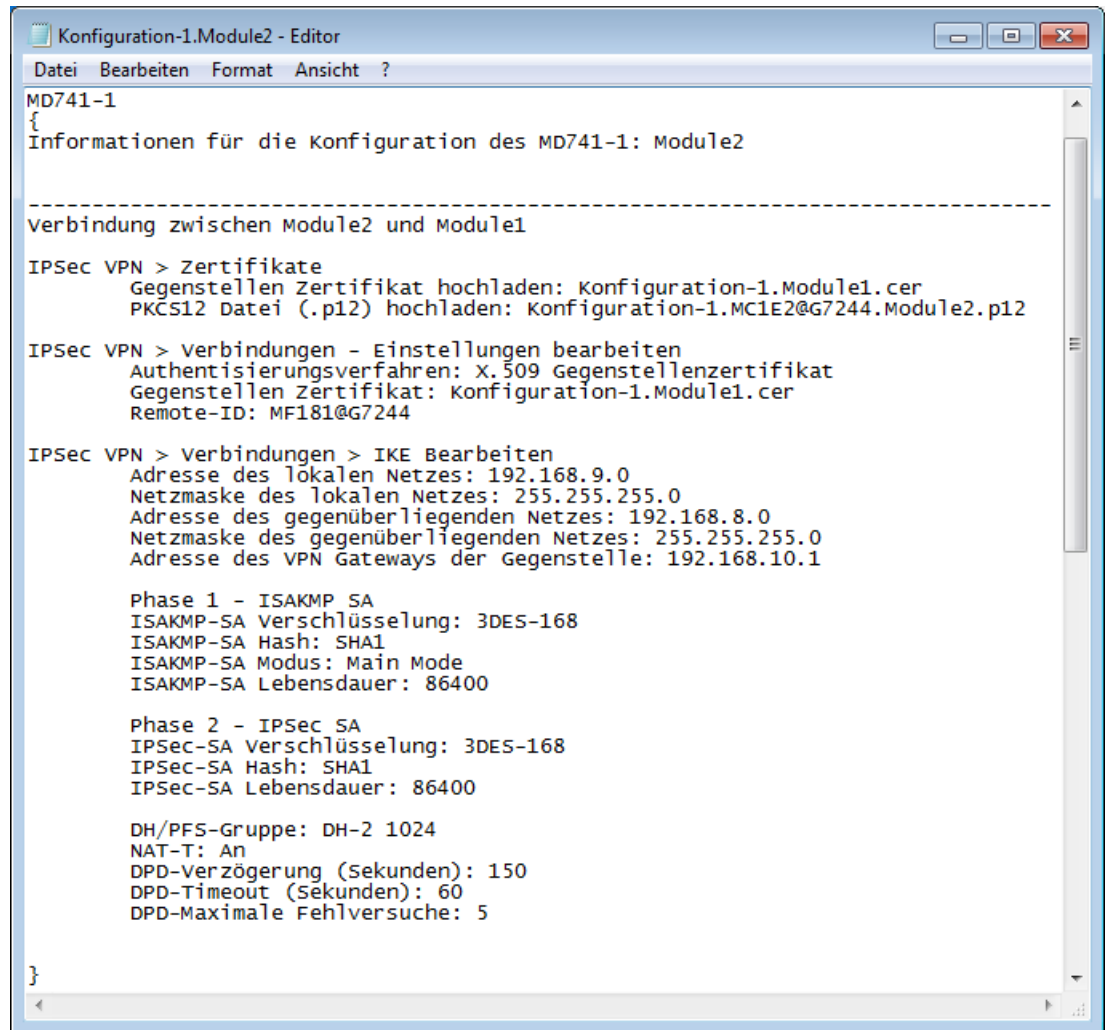
Übertragung an ein Modul

Sie können die VPN-Informationen zur Parametrierung eines SCALANCE M mit dem Security Configuration Tool generieren. Mit den generierten Dateien können Sie dann das SCALANCE M konfigurieren.

Folgende Dateitypen werden erzeugt:

- Exportdatei mit den Konfigurationsdaten
 - Dateityp: *.txt-Datei im ASCII-Format
 - Enthält die exportierten Konfigurationsinformationen für das SCALANCE M einschließlich einer Information über die zusätzlich erzeugten Zertifikate.
- Modul-Zertifikat
 - Dateityp: *.p12-Datei
 - Die Datei enthält das Modulzertifikat und das Schlüsselmateriale.
 - Der Zugriff ist passwortgeschützt.
- Gruppen-Zertifikat
 - Dateityp: *.cer-Datei

Die Konfigurationsdateien für das SCALANCE M können auch genutzt werden, um weitere VPN-Clienttypen, die nicht in der Modulauswahl enthalten sind, zu konfigurieren. Voraussetzung für die Verwendung dieser VPN-Clients ist die Unterstützung von IPsec-VPNs im Tunnelmodus.



```
MD741-1
{
Informationen für die Konfiguration des MD741-1: Module2

-----
Verbindung zwischen Module2 und Module1

IPsec VPN > Zertifikate
    Gegenstellen Zertifikat hochladen: Konfiguration-1.Module1.cer
    PKCS12 Datei (.p12) hochladen: Konfiguration-1.MC1E2@G7244.Module2.p12

IPsec VPN > Verbindungen - Einstellungen bearbeiten
    Authentisierungsverfahren: X.509 Gegenstellenzertifikat
    Gegenstellen Zertifikat: Konfiguration-1.Module1.cer
    Remote-ID: MF181@G7244

IPsec VPN > Verbindungen > IKE Bearbeiten
    Adresse des lokalen Netzes: 192.168.9.0
    Netzmaske des lokalen Netzes: 255.255.255.0
    Adresse des gegenüberliegenden Netzes: 192.168.8.0
    Netzmaske des gegenüberliegenden Netzes: 255.255.255.0
    Adresse des VPN Gateways der Gegenstelle: 192.168.10.1

    Phase 1 - ISAKMP SA
    ISAKMP-SA Verschlüsselung: 3DES-168
    ISAKMP-SA Hash: SHA1
    ISAKMP-SA Modus: Main Mode
    ISAKMP-SA Lebensdauer: 86400

    Phase 2 - IPsec SA
    IPsec-SA Verschlüsselung: 3DES-168
    IPsec-SA Hash: SHA1
    IPsec-SA Lebensdauer: 86400

    DH/PFS-Gruppe: DH-2 1024
    NAT-T: An
    DPD-Verzögerung (Sekunden): 150
    DPD-Timeout (Sekunden): 60
    DPD-Maximale Fehlversuche: 5

}
```

Bild 2-1 Export-Datei für SCALANCE M

Hinweis

Konfigurationsdateien werden nicht an das Modul übertragen. Es wird eine ASCII-Datei generiert, mit der Sie das SCALANCE M konfigurieren können. Dazu muss sich das Modul in mindestens einer VPN-Gruppe mit einem Security-Modul oder einem SOFTNET Security Client ab V3.0 befinden.

Gehen Sie so vor

1. Markieren Sie im Inhaltbereich das Modul "SCALANCE M".
2. Wählen Sie den Menübefehl "Übertragen" > "An Modul(e)..."

2.6 Benutzer verwalten

3. Geben Sie im folgenden Speicherdialog den Pfad- und Dateinamen der Konfigurationsdatei an und klicken Sie auf die Schaltfläche "Speichern".
4. Geben Sie im folgenden Dialog an, ob für die beiden erstellten Zertifikatsdateien ein eigenes Passwort erstellt werden soll.

Wenn Sie "Nein" wählen, wird als Passwort der Name der Projektierung vergeben (z. B. DHCP_ohne_Routing_02), nicht das Projektpasswort.

Wenn Sie "Ja" wählen (empfohlen), müssen Sie im darauf folgenden Dialog ein Passwort vergeben.

Ergebnis: Die Dateien (und Zertifikate) werden in dem von Ihnen angegebenen Verzeichnis abgespeichert.

Hinweis

Weitere Informationen zur Konfiguration finden Sie in den Betriebsanleitungen zum SCALANCE M87x und MD74x.

2.6 Benutzer verwalten

2.6.1 Übersicht zur Benutzerverwaltung

Wie ist die Benutzerverwaltung aufgebaut?

Der Zugriff auf die Security-Konfiguration wird durch konfigurierbare Benutzereinstellungen verwaltet. Richten Sie Benutzer mit jeweils einem Passwort zur Authentifizierung ein. Dem Benutzer weisen Sie eine systemdefinierte oder benutzerdefinierte Rolle zu. Den Rollen sind projektierungs- und baugruppenspezifische Rechte zugewiesen. Beachten Sie beim Anlegen die angegebenen Mengengerüste (Seite 18).

Bereits vorhandene Benutzer aus STEP 7 nach SCT migrieren

S7-CP

Bereits in STEP 7 angelegte Benutzer können nach SCT migriert werden. Dabei müssen Sie die Passwörter neu vergeben.

Detailinformationen dazu finden Sie in der Online-Hilfe.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen SCT-Dialog.



Eingabereihenfolge beim Anlegen Benutzern und Rollen

Wählen Sie eine der beiden Eingabereihenfolgen:

- Legen Sie zunächst einen neuen Benutzer an, legen Sie anschließend eine Rolle fest und weisen Sie im letzten Schritt dem Benutzer die Rolle zu.
- Definieren Sie zunächst eine neue Rolle, legen Sie anschließend einen Benutzer an und weisen Sie im letzten Schritt dem Benutzer die Rolle zu.

Benutzer-Authentifizierung

Die Benutzer des Projektes müssen sich beim Zugriff authentifizieren. Für jeden Benutzer müssen Sie deshalb eine Passwort-Authentifizierung festlegen.

ACHTUNG

Verwahren Sie Ihre Benutzer-Passwörter sicher

Vergessen Sie Ihre Benutzer-Passwörter, haben Sie keinen Zugriff mehr auf das betreffende Projekt und seine Konfigurationen sowie die Security-Module.

Zugriff auf Security-Module können Sie sich dann nur verschaffen, indem Sie ein "Rücksetzen auf Werkseinstellungen" durchführen. Dabei verlieren Sie aber die Konfigurationen.

ACHTUNG

Werden die Authentisierungseinstellungen geändert, so müssen die Security-Module erst neu geladen werden, damit diese Einstellungen (z. B. neue Benutzer, Passwortänderungen) auf den Modulen aktiv werden.

2.6.2 Benutzer anlegen

So erreichen Sie diese Funktion

Menübefehl SCT: "Optionen" > "Benutzerverwaltung", Register "Benutzer".

Menübefehl STEP 7: "Benutzer" > "Start der Benutzerverwaltung", Schaltfläche "Ausführen".
Zusätzlich wird die Benutzerverwaltung aus einzelnen Registern aufgerufen.

Tabelle 2- 1 Angaben im Register "Benutzer"

Parameter	Bedeutung
Benutzername	Frei wählbarer Benutzername.
Rolle	Je nach getroffener Zuordnung.
Kommentar	Zusätzliche Kommentareingabe.

Tabelle 2- 2 Schaltflächen im Register "Benutzer"

Bezeichnung	Bedeutung / Auswirkung
Bearbeiten	Markieren Sie einen Eintrag und klicken Sie auf die Schaltfläche. Im aufgeblendeten Dialog ändern Sie Benutzernamen, Passwort und Rolle.
Hinzufügen	Fügen Sie über die Schaltfläche einen neuen Benutzer ein. Im aufgeblendeten Dialog geben Sie den Benutzernamen ein und legen das Passwort und die system- oder benutzerdefinierte Rolle fest.
Löschen	Löschen Sie über die Schaltfläche den ausgewählten Eintrag. Hinweis Im Projekt muss immer mindestens ein Benutzer mit der Rolle "Administrator" vorhanden sein. Der Administrator, der bei Projekterstellung automatisch angelegt wird, kann nur gelöscht werden, solange mindestens ein weiterer Benutzer mit vollständigen Projektierungsrechten existiert.

2.6.3 Rollen anlegen

Welche Rollen gibt es?

Sie können einem Benutzer eine systemdefinierte oder benutzerdefinierte Rolle zuweisen. Die Rechte der Rolle legen Sie pro Security-Modul fest.

Systemdefinierte Rollen

Vordefiniert sind folgende systemdefinierten Rollen. Den Rollen sind bestimmte Rechte zugewiesen, die auf allen Baugruppen gleich sind und die der Administrator nicht ändern oder löschen kann.

- administrator

Standardrolle beim Anlegen eines SCT-Projekts.

Uneingeschränkte Zugriffsrechte auf alle Konfigurationsdaten.

- standard

Alle Rechte außer Benutzer/Rollen verwalten.

- diagnostics
Standardrolle beim Anlegen eines neuen Benutzers.
 - Lesender Zugriff auf Konfigurationen.
 - Lesender Zugriff auf das Security-Modul in der Betriebsart "Online" für Test und Diagnose.
- remote access
Keine Rechte außer Anmeldung an der Internetseite für benutzerspezifische Firewall-Regeln. Weitere Informationen finden Sie im Kapitel Benutzerspezifische Firewall-Regeln (Seite 110).

Bestehende SCT-Benutzer migrieren

Bei der Migration werden bestehende SCT-Benutzer den folgenden systemdefinierten Rollen zugeordnet.

- Bestehende Benutzer der Rolle "Admin" werden der systemdefinierten Rolle "administrator" zugeordnet.
- Bestehende Benutzer der Rolle "User" werden der systemdefinierten Rolle "diagnostics" zugeordnet.

Benutzerdefinierte Rolle

Zusätzlich zu den systemdefinierten Rollen können Sie benutzerdefinierte Rollen anlegen. Für eine benutzerdefinierte Rolle wählen Sie die Projektierungs- bzw. Baugruppenrechte und legen für jedes im Projekt verwendete Security-Modul die entsprechenden Rechte fest. Die benutzerdefinierten Rollen weisen Sie dem entsprechenden Benutzer manuell zu.

So erreichen Sie diese Funktion

Menübefehl SCT: "Optionen" > "Benutzerverwaltung...", Register "Rollen".

Menübefehl STEP 7: "Benutzer" > "Start der Benutzerverwaltung", Schaltfläche "Ausführen".
Zusätzlich wird die Benutzerverwaltung aus einzelnen Registern aufgerufen.

Tabelle 2- 3 Angaben im Register "Rollen"

Parameter	Bedeutung
Rollenname	Frei wählbarer Rollenname.
Kommentar	Zusätzliche Kommentareingabe.

Tabelle 2- 4 Schaltflächen im Register "Rollen"

Bezeichnung	Bedeutung / Auswirkung
Bearbeiten	Markieren Sie in der Liste eine benutzerdefinierte Rolle und klicken Sie auf die Schaltfläche. Im aufgeblendeten Dialog ändern Sie den Rollennamen und die der Rolle zugewiesenen Rechte. Systemdefinierte Rollen können nicht bearbeitet werden.
Hinzufügen	Fügen Sie über die Schaltfläche eine neue benutzerdefinierte Rolle hinzu. Im aufgeblendeten Dialog geben Sie den Rollennamen ein und weisen der Rolle aus der Rechteliste die entsprechenden Rechte zu. Angezeigt werden die Rechte der in der Rechtevorlage ausgewählten systemdefinierten Rolle.
Löschen	Löschen Sie über die Schaltfläche den ausgewählten Eintrag. Hinweis • Eine bereits erzeugte benutzerdefinierte Rolle kann nur gelöscht werden, wenn sie keinem Benutzer mehr zugewiesen ist. Weisen Sie dem Benutzer gegebenenfalls eine andere Rolle zu. • Systemdefinierte Rollen können nicht gelöscht werden.

2.6.4 Rechte verwalten

So erreichen Sie diese Funktion

Menübefehl SCT: "Optionen" > "Benutzerverwaltung...", Register "Rollen", Schaltfläche "Bearbeiten..." bzw. "Hinzufügen..."

Menübefehl STEP 7: "Benutzer" > "Start der Benutzerverwaltung", Schaltfläche "Ausführen". Zusätzlich wird die Benutzerverwaltung aus einzelnen Registern aufgerufen.

Benutzerdefinierte Rolle erstellen und zuweisen

1. Geben Sie einen Rollennamen ein.
2. Wählen Sie aus der Rechtevorlage eine systemdefinierte Rolle aus. Benutzerdefinierte Rollen werden in der Auswahl nicht angezeigt.

Ergebnis: Entsprechend der ausgewählten Rolle werden für jedes im Projekt verwendeten Security-Modul in der Rechteliste die dazugehörigen Rechte angezeigt. Die Rechte der nicht im Projekt verwendeten Security-Module sind ausgegraut.
3. Aktivieren bzw. deaktivieren Sie für jedes Security-Modul die Rechte, die der benutzerdefinierten Rolle zugewiesen werden sollen.
4. Klicken Sie auf die Schaltfläche "Übernehmen" um die Auswahl zu speichern bzw. "OK" um zu speichern und das Fenster zu schließen.
5. Weisen Sie die Rolle einem Benutzer zu.

Rollenrecht einer Baugruppe kopieren

Wählen Sie im Kontextmenü eines Security-Moduls aus der Objektliste den Befehl "Rechte kopieren" und weisen Sie diese über den Befehl "Rechte einfügen" einer anderen Baugruppe zu.

Projektierungsrechte

Je nach Benutzertyp stehen Ihnen pro Security-Projekt die folgenden Projektierungsrechte zur Auswahl:

Tabelle 2- 5 Projektierungsrechte für alle Security-Module

Projektierungsrecht	administrator	standard	diagnostics
Security diagnostizieren	x	x	x
Security konfigurieren	x	x	-
Benutzer und Rollen verwalten	x	-	-

Baugruppenrechte

In der Spalte "Service" wird das System angezeigt, auf welches das jeweilige Recht Auswirkungen hat.

Je nach Benutzertyp stehen Ihnen pro Security-Projekt die folgenden Baugruppenrechte zur Auswahl:

2.6 Benutzer verwalten

Tabelle 2- 6 Baugruppenrechte CP x43-1 Adv.

Recht innerhalb des Service	administrator	standard	diagnostics	Service
Web: CP-Dateisystem formatieren *	x	-	-	Dateisystem
FTP: Dateien vom CP-Dateisystem lesen **	x	x	x	
FTP: Dateien auf das CP-Dateisystem schreiben	x	x	-	
FTP: Dateien (DBs) von der S7-CPU lesen **	x	x	x	SPS
FTP: Dateien (DBs) in die S7-CPU schreiben ***	x	x	-	
Applet: Variablen über projektierte Symbole lesen *	x	x	x	
Applet: Variablen über projektierte Symbole schreiben *				
Applet: Variablen über absolute Adressen lesen *	x	x	x	
Applet: Variablen über absolute Adressen schreiben *	x	x	-	
Applet: Status der Baugruppen im Rack lesen *	x	x	x	
Applet: Bestellnummer der Baugruppen im Rack lesen *	x	x	x	
SNMP: MIB-II lesen	x	x	x	SNMP
SNMP: MIB-II schreiben	x	x	-	
SNMP: Automation-MIB lesen	x	x	x	
SNMP: LLDP-MIB lesen	x	x	x	
SNMP: SNMPv2-MIB lesen	x	x	x	
SNMP: MRP-MIB lesen	x	x	x	
SNMP: MRP-MIB schreiben	x	x	-	
SCT: Diagnose der Security-Baugruppe durchführen ****	x	x	x	Sicherheit
Web: IP Access Control-Liste erweitern *	x	-	-	
Web: Auf Web-Diagnose und CP-Dateisystem zugreifen	x	x	x	Web
Web: Testmail versenden *	x	x	x	
Web: Firmware aktualisieren *	x	x	-	Wartung
Web: Nachladen von Diagnosetexten *	x	x	-	

* Um die Funktion anzuwenden, muss das Gerätereicht "Web: Auf Web-Diagnose und CP-Dateisystem zugreifen" ebenfalls aktiviert sein.

** Um die Funktion anzuwenden, muss das Gerätereicht "FTP: Dateien vom CP-Dateisystem lesen" ebenfalls aktiviert sein.

*** Um die Funktion anzuwenden, muss das Gerätereicht "FTP: Dateien auf das CP-Dateisystem schreiben" ebenfalls aktiviert sein.

**** Um die Funktion anzuwenden, muss das Projektierungsrecht "Security diagnostizieren" ebenfalls aktiviert sein.

Tabelle 2- 7 Baugruppenrechte CP 1628

Recht innerhalb des Service	administrator	standard	diagnostics	Service
SNMP: MIB-II lesen	x	x	x	SNMP
SNMP: MIB-II schreiben	x	x	-	
SNMP: Automation-MIB lesen	x	x	x	
SNMP: SNMPv2-MIB lesen	x	x	x	
SCT: Diagnose der Security-Baugruppe durchführen	x	x	x	Sicherheit

 Tabelle 2- 8 Baugruppenrechte SCALANCE S $\geq$ V3.0

Recht innerhalb des Service	administrator	standard	diagnostics	Service
SNMP: MIB-II lesen	x	x	x	SNMP
SNMP: MIB-II schreiben	x	x	-	
SNMP: Automation-MIB lesen	x	x	x	
SNMP: SNMPv2-MIB lesen	x	x	x	
SNMP: MRP-MIB lesen	x	x	x	
SNMP: MRP-MIB schreiben	x	x	-	
SCT: Diagnose der Security-Baugruppe durchführen	x	x	x	Sicherheit
Laden der Konfigurationsdateien	x	x	-	
Web: Firmware aktualisieren	x	x	-	Wartung

Tabelle 2- 9 Baugruppenrechte SCALANCE S < V3.0

Recht innerhalb des Service	administrator	standard	diagnostics	Service
Laden der Konfigurationsdateien	x	x	-	Sicherheit
SCT: Diagnose der Security-Baugruppe durchführen	x	x	x	

2.7 Zertifikate verwalten

2.7.1 Übersicht

Wie verwalten Sie Zertifikate?

Im Zertifikatsmanager erhalten Sie eine Übersicht aller im Projekt verwendeten Zertifikate / CA-Zertifikate mit Angaben zu Antragssteller, Aussteller, Gültigkeit, Verwendung in SCT und Vorhandensein eines privaten Schlüssels.

Das CA-Zertifikat ist ein durch eine Zertifizierungsstelle, die so genannte "Certificate Authority", ausgestelltes Zertifikat, von denen die Gerätezertifikate abgeleitet werden. Dazu gehören die SSL-Zertifikate, die zur Authentifizierung bei der Online-Kommunikation zwischen einem Gerät und einem Security-Modul benötigt werden. Zertifizierungsstellen können sein:

- SCT selbst. Sind "Antragsteller" und "Aussteller" gleich, dann handelt es sich um ein selbst-signiertes, also durch SCT ausgestelltes Zertifikat.
- Eine übergeordnete Zertifizierungsstelle. Diese projektexternen Fremdzertifikate werden importiert und im Zertifikatsspeicher von SCT abgelegt.

Zertifikate, die von einer der beiden Zertifizierungsstellen angelegt werden, haben immer einen privaten Schlüssel, damit die Gerätezertifikate abgeleitet werden können.

Zusätzlich stehen Ihnen im Zertifikatsmanager die folgenden Funktionen zur Auswahl:

- Ändern von bestehenden Zertifikaten (z. B. Gültigkeitsdauer).
- Importieren von neuen Zertifikaten und Zertifizierungsstellen.
- Importieren von FTPS-Zertifikaten. S7-CP
- Exportieren der im Projekt verwendeten Zertifikate und Zertifizierungsstellen.
- Erneuern von abgelaufenen Zertifikaten und Zertifizierungsstellen.
- Ersetzen bestehender Zertifizierungsstellen durch andere.

Hinweis

Laden der Projekte

Nach dem Ersetzen oder Erneuern von Zertifikaten muss das Projekt auf das entsprechende Security-Modul geladen werden.

Nach dem Ersetzen oder Erneuern von CA-Zertifikaten muss das Projekt auf alle Security-Modul geladen werden.

ACHTUNG**Aktuelles Datum und aktuelle Uhrzeit auf den Security-Modulen**

Achten Sie bei der Verwendung von gesicherter Kommunikation (z. B. HTTPS, VPN...) darauf, dass die betroffenen Security-Module über die aktuelle Uhrzeit und das aktuelle Datum verfügen. Die verwendeten Zertifikate werden sonst als nicht gültig ausgewertet und die gesicherte Kommunikation funktioniert nicht.

So erreichen Sie diese Funktion

Menübefehl SCT: "Optionen" > "Zertifikatsmanager...".

In den einzelnen Registern stehen Ihnen die folgenden Schaltflächen zur Verfügung:

Schaltfläche	Beschreibung
Importieren / Exportieren	Import / Export von Gerätezertifikaten bzw. CA-Zertifikaten, die nicht in SCT angelegt wurden. Die Zertifikate werden auf das Security-Modul übertragen. Folgende Formate sind erlaubt: *.pem (nur Zertifikat) *.crt (nur Zertifikat) *.p12 (Zertifikat mit dazugehörigem privaten Schlüssel) Hinweis - Benutzer mit der Rolle "Diagnose" dürfen keinen Export durchführen.
Anzeigen	Öffnet den Zertifikatsdialog von Windows, in dem Sie eine Übersicht aller Zertifikatsdaten angezeigt bekommen.

Register "Zertifizierungsstellen"

Die hier angezeigten Zertifikate werden durch eine Zertifizierungsstelle angelegt.

- CA-Zertifikate eines Projekts: Beim Erstellen eines neuen SCT-Projekts wird für das Projekt ein CA-Zertifikat erzeugt. Von diesem Zertifikat werden die SSL-Zertifikate für die einzelnen Security-Module abgeleitet.
- CA-Gruppenzertifikate: Beim Erstellen einer neuen VPN-Gruppe wird für die Gruppe ein CA-Zertifikat erzeugt.

Register "Gerätezertifikate"

Anzeige der gerätespezifischen Zertifikate, die von SCT für ein Security-Modul erzeugt werden. Dazu gehören:

- **SSL-Zertifikate:** Für jedes angelegte Security-Modul wird ein SSL-Zertifikat erzeugt, das aus einem CA-Zertifikat des Projekts abgeleitet ist. SSL-Zertifikate werden zur Authentifizierung bei der Kommunikation zwischen PG/PC und Security-Modul, beim Laden der Konfiguration (nicht für CPs) sowie beim Logging herangezogen.
- **Gruppenzertifikate:** Zusätzlich wird für jedes Security-Modul pro VPN-Gruppe, in der es sich befindet, ein Gruppenzertifikat erzeugt.

Register "Vertrauenswürdige Zertifikate und Stammzertifizierungsstellen"

Anzeige der in SCT importierten Fremdzertifikate. Importiert werden können z. B. Server-Zertifikate von externen FTP-Servern oder Projektzertifikate von anderen SCT-Projekten.

CP

Das importierte Fremdzertifikat wird auf alle im SCT-Projekt verwalteten CPs übertragen. Mit diesem Zertifikat kann sich das Security-Modul dann z. B. beim Zugriff auf einen FTPS-Server ausweisen. Die SCT-Projektierung selbst verwendet das importierte Zertifikat nicht.

SCA

Anzeige der Zertifizierungsstellen, die für die Verifizierung der Security-Module durch externe Dienste wie DynDNS notwendig sind.

2.7.2 Zertifikate erneuern

Bedeutung

In diesem Dialog erneuern Sie Zertifikate und CA-Zertifikate. Sie können bei Bedarf, z. B. bei kompromittierten Zertifikaten, ein Zertifikat importieren oder ein neues Zertifikat vom Security Configuration Tool erzeugen lassen.

So erreichen Sie diese Funktion

1. Klicken Sie mit der rechten Maustaste auf einen Listeneintrag im Zertifikatsmanager.

2. Wählen Sie den Eintrag "Zertifikat erneuern...".

Neues Zertifikat erstellen

Zertifizierungsstelle
Wählen Sie, wie das neue Zertifikat signiert werden soll:

☒ Selbst-signiert
☐ Signiert von einer Zertifizierungsstelle

Name der Zertifizierungsstelle:

Zertifikatsparameter
Geben Sie die Parameter für das neue Zertifikat ein:

Antragsteller:

Gültig von:

Gültig bis:

Alternativer Antragstellername:

3. Wählen Sie aus, ob das neue Zertifikat selbst-signiert oder durch eine Zertifizierungsstelle signiert werden soll.
4. Wenn das Zertifikat durch eine Zertifizierungsstelle signiert werden soll, wählen Sie über die Schaltfläche "Auswählen..." die zu verwendende Zertifizierungsstelle aus. Zur Auswahl stehen dabei nur Zertifizierungsstellen, die im Zertifikatsspeicher des aktuellen SCT-Projekts abgelegt sind.
5. Wählen Sie einen Zeitraum aus, in dem das Zertifikat gültig ist. Standardmäßig wird in das Feld "Gültig von:" die aktuelle Zeit und in das Feld "Gültig bis:" der Wert vom aktuellen Zertifikat eingetragen.
6. Geben Sie je nach Zertifikat die folgenden Werte ein:

Zu erneuerndes Zertifikat	Parameter	
	Antragssteller	Alternativer Antragstellername
CA-Zertifikate des Projekts	Name des CA-Zertifikats	-
CA-Gruppenzertifikat	Name des CA-Gruppenzertifikats	-
SSL-Zertifikat für S7-CP	Name des Security-Moduls	IP-Adressen der Gigabit und PROFINET-Schnittstelle, durch ein Komma getrennt.
SSL-Zertifikat für PC-CP	Name des Security-Moduls	IP-Adresse des Security-Moduls.
SSL-Zertifikat für SCALANCE S, SCALANCE M und SOFTNET Security Client	Name des Security-Moduls	-
Gruppenzertifikat des Security-Moduls	Name des Gruppenzertifikats	Von der CA abgeleitet.

Zusätzliche Parameter konfigurieren

Klicken Sie auf die Schaltfläche "Zusätzliche Parameter konfigurieren", um Daten wie die E-Mail-Adresse zu hinterlegen.

2.7.3 Zertifikate ersetzen

Bedeutung

In dem Dialog ersetzen Sie das bestehende CA-Zertifikat des Projekts oder CA-Gruppenzertifikat durch ein neues.

So erreichen Sie diese Funktion

1. Klicken Sie mit der rechten Maustaste auf einen Listeneintrag im Register "Zertifizierungsstellen".
2. Wählen Sie den Eintrag "Zertifikat ersetzen...".
3. Der Dialog "Zertifizierungsstelle austauschen" wird geöffnet.

Alle im Feld "Betroffene Zertifikate" aufgelisteten Zertifikate werden neu abgeleitet. Somit kann das CA-Gruppenzertifikat einer bereits projektierte VPN-Gruppe innerhalb des SCT-Projekts durch das CA-Gruppenzertifikat eines anderen SCT-Projekts ersetzt werden. Die Gruppenzertifikate für die VPN-Gruppenteilnehmer werden also in beiden Projekten von dem gleichen CA-Gruppenzertifikat abgeleitet.

Falls beim Schließen des Zertifikatmanagers ein Hinweisdialog erscheint, laden Sie die geänderte Konfiguration erneut auf das Security-Modul.

Welches Format darf das Zertifikat haben?

Von der importierten CA werden weitere Zertifikate in SCT abgeleitet. Deshalb können Sie nur Zertifikate mit privatem Schlüssel auswählen:

- *.p12

Module anlegen und Netzparameter einstellen

Das vorliegende Kapitel macht Sie damit vertraut, wie Module angelegt werden und welche Einstellungen für die einzelnen Module in einem Projekt möglich sind. Hierbei spielen die Einstellungen für die Firewall-Funktion und NAT/NAPT-Router-Funktion der Security-Module die Hauptrolle.

Hinweis



Die Firewall-Einstellungen, die Sie für die einzelnen Module vornehmen können, können auch die Kommunikation beeinflussen, die über IPsec-Tunnelverbindungen im internen Netz (VPN) abgewickelt wird.

Weitere Informationen

Wie Sie IPsec-Tunnel konfigurieren, wird ausführlich im nächsten Kapitel dieses Handbuches erläutert.



Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen SCT-Dialog.

ACHTUNG

Leistungsmerkmale und Gerätetypen

Beachten Sie bei dem von Ihnen verwendeten Gerätetyp, welche Funktionen jeweils unterstützt werden.

Siehe auch

Online Funktionen - Test, Diagnose und Logging (Seite 203)

Module in SCT anlegen - So erreichen Sie diese Funktion

1. Selektieren Sie im Navigationsbereich das Objekt "Alle Module".

2. Wählen Sie den Menübefehl "Einfügen" > "Modul".

Auswahl einer Baugruppe oder Softwarekonfiguration

Produkttyp

- ☒ SCALANCE S
- ☐ SOFTNET Configuration (SOFTNET Security Client, SCALANCE M87x/MD74x)

Baugruppe

- ☐ S602
- ☒ S612
- ☐ S613

Firmwarerelease

- ☒ V3
- ☐ V2
- ☐ V1

Konfiguration

Name des Moduls:

MAC-Adresse:

IP-Adresse (ext.): Subnetzmaske (ext.):

☐ Routing aktivieren

IP-Adresse (int.): Subnetzmaske (int.):

Kurzbeschreibung

SCALANCE S612 Modul (6GK5 612-0BA10-2AA3) zum Schutz von Geräten und Netzen in der Automatisierungstechnik und zur Sicherung der industriellen Kommunikation.
Funktionen: VPN (128 Tunnel parallel), Stateful Inspection Firewall, Adressumsetzung (NAT / NAPT), Syslog, symbolische Namen, PPPoE, DynDNS, SNMP, benutzerspezifische Firewall-Regeln.

☐ Auswahl speichern

OK Abbrechen Hilfe

3. Nehmen Sie die folgenden Einstellungen vor. Die Adressparameter im Feld "Konfiguration" können Sie auch im Inhaltsbereich eintragen bzw. verändern. Information dazu finden Sie im Kapitel Parameter im Inhaltsbereich (Seite 75).

Parameter	Bedeutung
Produkttyp	Produkttyp, der beim Anlegen eines neuen Moduls verwendet wird. SCALANCE S SOFTNET Configuration (SOFTNET Security Client, SCALANCE M87x/MD74x)
Baugruppe	Je nach Auswahl des Produkttyps können Sie hier den Baugruppentyp angeben, der beim Anlegen eines neuen Moduls verwendet wird. Wählen Sie die Auswahl "VPN Client", um ein VPN-fähiges Produkt von einem anderen Hersteller einzufügen. Hinweis Ob die ausgeleitete Konfigurationsdatei funktioniert, hängt vom jeweiligen Partnerprodukt ab.
Firmwarerelease	Für die SCALANCE S-Module und den SOFTNET Security Client können hier die Firmware / Softwarestände angegeben werden.
Name des Moduls	Frei wählbarer Name des Moduls.
MAC-Adresse	Hinweis zum Aufbau der MAC-Adresse: Die MAC-Adresse besteht aus einem festen und einem variablen Teil. Der feste Teil ("Basis-MAC-Adresse") kennzeichnet den Hersteller (Siemens, 3COM, ...). Der variable Teil der MAC-Adresse unterscheidet die verschiedenen Ethernet-Teilnehmer.
IP-Adresse (ext.)	IP-Startadresse für das externe Interface. Format / Wertebereich für IP-Adresse Die IP-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.80.0.16
Subnetzmaske (ext.)	Wertebereich für Subnetzmaske. Wird entsprechend der eingegebenen IP-Adresse vorgeschlagen. Die Subnetzmaske besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 255.255.0.0
Routing aktivieren	Wenn Sie diese Option aktivieren, befindet sich das Security-Modul im Routing-Modus.
IP-Adresse (int.) nur anzugeben, wenn Routing-Modus aktiviert	IP-Startadresse für die interne Schnittstelle. Die IP-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.80.0.17

Parameter	Bedeutung
Subnetzmaske (int.) nur anzugeben, wenn Routing-Modus aktiviert	Wertebereich für Subnetzmaske. Die Subnetzmaske wird entsprechend der eingegebenen IP-Adresse vorgeschlagen. Die Subnetzmaske besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 255.255.0.0
Auswahl speichern	Aktivieren Sie diese Funktion, wird Ihre derzeit eingestellte Konfiguration in die Standard-Initialisierungswerte übernommen. Beim Einfügen von neuen Modulen wird nicht mehr der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" geöffnet, sondern gleich ein Modul entsprechend den festgelegten Einstellungen in das Projekt eingefügt. Um diese Funktion wieder aufzuheben und einen anderen Modultyp auszuwählen, müssen Sie diese Funktion unter folgendem Menüpfad deaktivieren: "Projekt" > "Eigenschaften..." > "Standard-Initialisierungswerte"

Hinweis

Zusätzliche Einstellungen

S≥V3.0

Porteinstellungen, Festlegungen zum DMZ-Port, Aktivierung von PPPoE usw. nehmen Sie im Register "Schnittstellen" vor. Informationen dazu finden Sie im Kapitel Schnittstellen konfigurieren (SCALANCE S) (Seite 77).

CPs in STEP 7 anlegen

CPs werden nur in STEP 7 angelegt. Sie erscheinen nach dem Anlegen und der Festlegung als Security-Modul in deren Eigenschaften in der Liste der konfigurierten Module in SCT. Die Adressdaten werden aus STEP 7 übernommen und können in SCT nicht geändert werden.

Siehe auch

Wertebereiche IP-Adresse, Subnetzmaske und Adresse des Netzübergangs (Seite 215)

MAC-Adresse (Seite 216)

3.1 Parameter im Inhaltsbereich

So erreichen Sie die Ansicht

Selektieren Sie im Navigationsbereich das Objekt "Alle Module".

Folgende Eigenschaften der Module werden spaltenweise angezeigt:

Eigenschaft/Spalte	Bedeutung	Kommentar/Auswahl
Nummer	Fortlaufende Modulnummer	wird automatisch vergeben
Name	Eindeutige Modulbenennung.	frei wählbar
Typ	Gerätetyp	Hinweis Für Geräte vom Produkttyp "SOFNET Configuration" existiert kein Eigenschaftsdialog. Für SCALANCE M können Sie im Inhaltsbereich nur die IP-Adressen und die Subnetzmasken einstellen.
IP-Adresse ext.	IP-Adresse, über die das Gerät im externen Netz erreichbar ist, z. B. zum Laden der Konfiguration.	Im Netzwerk passende Vergabe.
Subnetzmaske ext.	Subnetzmaske	Im Netzwerk passende Vergabe.
IP-Adresse int.	IP-Adresse, über die das Gerät im internen Netz erreichbar ist, wenn es als Router konfiguriert ist.	Im Netzwerk passende Vergabe. Das Eingabefeld ist nur dann editierbar, wenn der Routing-Modus aktiviert ist.
Subnetzmaske int.	Subnetzmaske	Im Netzwerk passende Vergabe. Das Eingabefeld ist nur dann editierbar, wenn der Routing-Modus aktiviert ist.
Standard-Router	IP-Adresse des Standard-Routers.	Im Netzwerk passende Vergabe.
MAC-Adresse	Hardware-Adresse des Moduls.	Die MAC-Adresse ist auf dem Modulgehäuse aufgedruckt.
Kommentar	Technologisch sinnvolle Information zum Modul und das durch das Modul geschützte Subnetz.	frei wählbar

Adressparameter für SCALANCE S verändern

Für SCALANCE S können die Adressparameter im Inhaltsbereich eingegeben und verändert werden.

Bedeutung der Adressparameter für CPs

CP

Für die CPs werden die folgenden Adressen aus STEP 7 angezeigt:

Feld in SCT	CP x43-1	CP 1628
IP-Adresse ext.	IP-Adresse Gigabit	IP-Adresse IE (Industrial Ethernet)
IP-Adresse int.	IP-Adresse PROFINET	Wird nicht angezeigt
Subnetzmaske ext	Subnetzmaske Gigabit	Subnetzmaske IE
Subnetzmaske int.	Subnetzmaske PROFINET	Wird nicht angezeigt
MAC-Adresse	MAC-Adresse Gigabit	MAC-Adresse IE

Ebenfalls angezeigt werden die Adressdaten im Register "Schnittstellen".

Dynamisch vergebene IP-Adresse

S7-CP

Ist in STEP 7 projektiert, dass die IP-Adresse dynamisch vergeben werden soll, wird dies in SCT je nach Einstellungen folgendermaßen dargestellt:

Tabelle 3- 1 Gigabit-Schnittstelle

Betriebsart in STEP 7	IP-Adresse ext. / Subnetzmaske ext.
IP-Adresse von einem DHCP-Server beziehen	dynamisch

Tabelle 3- 2 PROFINET-Schnittstelle

Betriebsart in STEP 7	IP-Adresse ext. / Subnetzmaske int.
IP-Adresse von einem DHCP-Server beziehen	dynamisch
IP-Adresse im Anwenderprogramm einstellen	dynamisch
IP-Adresse auf anderem Weg einstellen	dynamisch

3.2 Schnittstellen konfigurieren (SCALANCE S)

3.2.1 Übersicht Ports

SCA.

Unterstützte Ports und Anschlussmöglichkeiten

Der SCALANCE S V3.0 unterstützt die folgenden Ports:

- Roter Port (eth0): Unsicheres Netzwerk
- Grüner Port (eth1): Gesichertes Netzwerk
- Gelber Port (eth2): DMZ (Demilitarisierte Zone) oder als Fernwartungszugang über PPPoE S623

Gelber Port als DMZ-Port

Eine DMZ wird genutzt, wenn Dienste für ein externes Netz bereitgestellt werden sollen und das interne Netz, das Daten für diese Dienste liefert, von dem externen Netz entkoppelt sein soll.

In der DMZ können z. B. Terminal-Server stehen, auf denen Wartungs- und Diagnose-Programme installiert sind, die definierte Zugriffe auf bestimmte Systeme im sicheren Netz erlauben. Zugriff haben nur zugelassene Benutzer oder Clients aus dem unsicheren Netz oder per VPN angeschlossene Clients.

Die Firewall-Regeln können so projektiert werden, dass vom Internet Zugriffe auf Geräte in der DMZ aber nicht auf das interne Netz am grünen Port möglich sind. Für erhöhten Schutz können erlaubte Zugriffe ausschließlich auf VPN-Datenverkehr eingeschränkt werden.

Um auch Geräten in der DMZ eine dynamische IP-Adresse zuweisen zu können, kann auf dem gelben Port ein DHCP-Server aktiviert werden. Allerdings muss in einem solchen Anwendungsfall dafür gesorgt werden, dass die Geräte in der DMZ per DHCP immer die gleiche IP-Adresse bekommen, da diese IP-Adressen bei der Firewall-Konfiguration zu benutzen sind. D.h. bei der DHCP-Projektierung darf nicht die dynamische Adressvergabe, sondern nur die statische Adressvergabe anhand der MAC-Adresse oder anhand der Client-ID verwendet werden.

Gelber Port als Fernwartungsport

Der gelbe Port kann als VPN-Endpunkt genutzt werden, um als Anschlussport für Fernwartungszwecke genutzt werden zu können. In Verbindung mit einem DSL-Modem wird der gelbe Port dann im PPPoE-Modus betrieben bzw. in Verbindung mit einem vorgeschalteten DSL-Router mit statischer IP-Adresse.

Point to Point Protocol over Ethernet

Zur Einwahl in das Internet / WAN wird PPPoE eingesetzt. PPPoE kann entweder am externen Port oder am DMZ-Port konfiguriert werden.

Einstellungen für den externen Port mit Adresse über PPPoE

Um einen Internet-/WAN-Anschluss direkt über ein DSL-Modem zu ermöglichen, erfolgt die Zuweisung der IP-Adresse am externen Port über PPPoE. Bei PPPoE handelt es sich um ein Einwahlprotokoll zum Bezug von IP-Adressen von einem Internet Service Provider (ISP). SCALANCE S wird dabei im Routing-Modus betrieben.

Hinweis

Ein projektierte Standard-Router wird bei Verwendung von PPPoE nicht berücksichtigt.

Funktionen der einzelnen Ports

Folgende Funktionen können auf den einzelnen Ports genutzt werden:

Funktion	Grün (intern)	Rot (extern)	Gelb	
			Betriebsmodus Fernwartung	Betriebsmodus DMZ
Statische IP-Adresse	x	x	-	x
Dynamische IP-Adresse (über PPPoE)	-	x	x	-
WAN-Zugang über DSL-Modem oder DSL-Router	-	x (wenn nicht auf gelbem Port)	x (wenn nicht auf rotem Port)	-
Bridge-Modus	x		-	
Routing Modus	x	x	x	
DHCP-Server	x	-	-	x
Fernwartung mit VPN	-	Mit DSL-Router	Mit DSL-Modem	Mit DSL-Router

3.2.2 Schnittstellen



Schnittstellenrouting - Auswahlmöglichkeiten

Wenn sich das Security-Modul in keiner VPN-Gruppe befindet, ist der Modus für das Schnittstellenrouting automatisch eingestellt und kann in diesem Feld verändert werden. Die Auswahl ist für Port 1 und Port 2 gültig.

Wenn sich das Security-Modul in einer VPN-Gruppe befindet, kann der Modus für das Schnittstellenrouting nicht verändert werden.

Bridge-Modus	Für den Betrieb in flachen Netzen. Externer und interner Port befinden sich im selben IP-Subnetz. Für S623: Der DMZ-Port muss sich in einem anderen Subnetz befinden oder steht im Betriebsmodus "Aus".
Routing-Modus	Alle Ports befinden sich in verschiedenen IP-Subnetzen. Hinweis Wenn Sie für das SCALANCE S-Modul den Routing-Modus aktiviert haben, können keine MAC-Firewall-Regeln definiert werden.

Eingabemöglichkeiten für statische Adresszuweisung

- IP-Adresse mit Subnetzmaske
- DNS-Server, wenn dynamisches DNS verwendet wird

Adresszuweisung über PPPoE

- IP-Adresse wird vom ISP vorgegeben

Auflösen von FQDN (Full Qualified Domain Name) in IP Adressen

Um FQDNs aufzulösen, werden DNS-Server benötigt, welche die entsprechende IP-Adresse zum FQDN zurück geben.

- Geben Sie bevorzugten und alternativen DNS-Server ein.
- IP-Zuweisung über PPPoE: Die DNS-Server können über PPPoE automatisch bezogen werden. Kann nur für den externen Port und den DMZ-Port im Betriebsmodus "Fernwartung" eingestellt werden.

Zusätzliche MAC-Adresse

Die zusätzlichen MAC-Adressen werden wie folgt abgeleitet:

- MAC-Adresse (intern) = aufgedruckte MAC-Adresse + 1
- MAC-Adresse (DMZ-Port) = aufgedruckte MAC-Adresse + 2

Beim Betrieb in flachen Netzen (Bridge-Modus) ist immer die aufgedruckte MAC-Adresse sowohl an der internen wie an der externen Schnittstelle gültig.

Zusätzliche Einstellungen für den DMZ-Port

S623

Der DMZ-Port routet immer zum externen und internen Port, auch wenn im Schnittstellenrouting Bridge-Modus ausgewählt ist.

Hinweis

Externer- und DMZ-Port als Internetzugang

Der gleichzeitige Betrieb von PPPoE am externen Port und im Betriebsmodus "Fernwartung" am DMZ-Port (Dual-ISP) ist nicht möglich.

Feld	Beschreibung
Betriebsmodus	Legen Sie fest, wie der DMZ-Port genutzt werden soll. Wählen Sie abhängig vom gewünschten Einsatz zwischen den folgenden Funktionen: - DMZ: Keine IP-Zuweisung über PPPoE möglich. - Fernwartung: Port ist über PPPoE direkt mit dem Internet (ISP) verbunden.
IP-Zuweisung	Beim Betriebsmodus "DMZ" erfolgt die IP-Zuweisung statisch. Im Betriebsmodus "Fernwartung" erfolgt die IP-Adresszuweisung durch den ISP.

Siehe auch

Dynamisches DNS (Seite 80)

3.2.3 Dynamisches DNS

S≥V3.0

Was ist Dynamisches DNS?

Mit Dynamischem DNS können Sie mit einem fest definierten Namen (FQDN) auf eine sich ständig ändernde IP-Adresse zugreifen. Dies ist notwendig, wenn Sie z. B. auf einen Server zugreifen möchten, der über eine öffentliche, sich ändernde IP Adresse erreichbar ist.

Wie funktioniert Dynamisches DNS?

Das Security-Modul meldet einem Provider für Dynamisches DNS (z. B. DynDNS.org, no-ip.com) die aktuelle WAN-IP, über die das Modul erreichbar ist. Der Provider sorgt dafür, dass DNS-Anfragen auf den FQDN des Modules mit der WAN-IP des Modules beantwortet werden.

Dynamisches DNS ist auf folgenden Ports zugelassen:

- Externer Port
- DMZ-Port im Betriebsmodus "Fernwartung"

Dynamisches DNS einrichten - Voraussetzungen

Voraussetzung:

- Bei einem der unterstützten Anbieter für Dynamisches DNS ist ein Account angelegt und ein FQDN registriert.
- Wenn sich das Security-Modul hinter einem DSL-Router befindet, muss im Register "Schnittstellen" ein gültiger DNS-Server eingetragen sein.

So erreichen Sie diese Funktion

1. Wählen Sie in den Moduleigenschaften des Security-Moduls das Register "Schnittstellen".
2. Klicken Sie auf die Schaltfläche "Erweiterte Einstellungen...".

3. Wählen Sie das Register "Dynamisches DNS".

Erweiterte Schnittstellen-Einstellungen : S623-V3, DMZ

Internet Verbindung | **Dynamisches DNS** | Port-Einstellungen

Primärer DynDNS-Dienst

☒ Service aktivieren ☒ Fehler bei Überprüfung des Server-Zertifikats ignorieren

Service Typ: DynDNS-HTTP

Provider: DynDNS.org

Provider Benutzer-Konto: mydyndnsaccount Provider Passwort:

FQDN: Hostname: device12282A Domain: dyndns.com

☒ IP-Adresswechsel auf DSL-Router überwachen Periode: 25 Minuten

Sekundärer DynDNS-Dienst

☐ Service aktivieren ☐ Fehler bei Überprüfung des Server-Zertifikats ignorieren

Service Typ: DynDNS-HTTP

Provider: no-ip.com

Provider Benutzer-Konto: Provider Passwort:

FQDN: Hostname: Domain:

☐ IP-Adresswechsel auf DSL-Router überwachen Periode: 20 Minuten

Benutzerdefinierte Einstellungen

Provider Aktualisierungs URL:

Check-IP Service URL:

OK Abbrechen Hilfe

4. Aktivieren Sie das Kontrollkästchen "Service aktivieren".

5. Nehmen Sie die folgenden Einstellungen vor.

Primären DynDNS-Dienst aktivieren

IP-Einstellungen	
Provider	Wählen Sie aus, bei welchem DynDNS-Anbieter Sie einen DynDNS-Account eingerichtet haben.
Provider-Benutzerkonto	Geben Sie den Benutzernamen ein, den Sie beim Anlegen des DynDNS-Accounts festgelegt haben.
Provider-Passwort	Geben Sie das Benutzerpasswort ein, das Sie beim Anlegen des DynDNS-Accounts festgelegt haben.
FQDN	Geben Sie den Hostnamen (z. B. www) und den Domainnamen (z. B. abc.de) ein, der beim DynDNS-Anbieter registriert ist.
IP-Adresswechsel auf DSL-Router überwachen	Ist das Security-Modul über einen DSL-Router mit dem Internet verbunden, wird durch Aktivieren der Funktion der Check-IP-Dienst aktiviert. Das Security-Modul sendet periodisch Anfragen zur Bestimmung der aktuellen IP-Adresse des DSL-Routers sowie zur Detektion eines IP-Adresswechsels auf dem DSL-Router. Geben Sie an, in welchem Zyklus der Check-IP-Dienst aufgerufen wird. Periode: 10 ... 1440 Minuten

Ergebnis: Nach der Eingabe steht in der Online-Ansicht statt dem eingegebenen Hostnamen immer die aktuelle, öffentliche IP-Adresse.

Sekundären DynDNS-Dienst aktivieren

Legen Sie für den Fall, dass der primäre Provider ausfällt, einen weiteren DynDNS-Update-Anbieter an. Nehmen Sie zusätzlich zu den Angaben im Feld "Primärer DynDNS-Service" die folgenden Eingaben vor:

IP-Einstellungen	
Provider Aktualisierungs-URL	Bei den vordefinierten Providern (DynDNS.org und No-IP.com) wird die URL vorausgefüllt.
Check IP-Service URL	Bei den vordefinierten Providern (DynDNS.org und No-IP.com) wird die URL vorausgefüllt.
Fehler bei Überprüfung des Server-Zertifikats ignorieren	Damit die Authentifizierungsdaten geschützt sind, wird das Zertifikat des DynDNS-Update-Servers standardmäßig überprüft. Schlägt die Prüfung des Zertifikates fehl, so wird die https-Verbindung beendet und die Account-Daten werden nicht übertragen. Wenn Sie das Kontrollkästchen aktivieren, wird die Funktion deaktiviert, z. B. wenn das Server-Zertifikat des DynDNS-Dienstes ungültig ist (z. B. abgelaufen).

3.2.4 Porteinstellungen

S≥V3.0

Ports konfigurieren

Nehmen Sie für die Ports die Verbindungseinstellungen vor.

- Halbduplex: Das Security-Modul kann zu einem Zeitpunkt entweder Daten empfangen oder senden.
- Vollduplex: Das Security-Modul kann zu einem Zeitpunkt gleichzeitig Daten empfangen und senden.

Übertragungsgeschwindigkeit und Duplex-Verfahren wählen

Gehen Sie folgendermaßen vor:

1. Wählen Sie in den Moduleigenschaften des Security-Moduls das Register "Schnittstellen".
2. Klicken Sie auf die Schaltfläche "Erweiterte Einstellungen...".
3. Wählen Sie das Register "Port Einstellungen".

Folgende Übertragungsraten werden unterstützt:

Auswahl	Beschreibung
Autonegotiation	Die Übertragungsgeschwindigkeit und das Duplex-Verfahren werden automatisch ausgewählt. Hinweis Nur wenn Autonegotiation ausgewählt ist, wird die Autocrossing-Funktion unterstützt.
10 MBit/s, half- und full-duplex	Übertragungsgeschwindigkeit von 10 Mbit/s.
100 MBit/s, half- und full-duplex	Übertragungsgeschwindigkeit von 100 Mbit/s.

3.2.5 Internetverbindung

S≥V3.0

Zusätzliche Parameter

Wenn eine Verbindung über PPPoE eingestellt ist, nehmen Sie Einstellungen zum ISP vor.

Gehen Sie folgendermaßen vor

1. Wählen Sie in den Moduleigenschaften des Security-Moduls das Register "Schnittstellen".
2. Wählen Sie für den DMZ-Port den Betriebsmodus "Fernwartung".
3. Klicken Sie auf die Schaltfläche "Erweiterte Einstellungen...".
4. Wählen Sie das Register "Internet Verbindung".
5. Nehmen Sie die folgenden Einstellungen vor:

Funktion	Beschreibung
Benutzername	Geben Sie den Namen zur Anmeldung beim ISP-Account ein.
Passwort	Geben Sie das Passwort zur Anmeldung beim ISP-Account ein.
Passwortbestätigung	Geben Sie das Passwort zur Anmeldung beim ISP-Account erneut ein.
Authentifizierung	Wählen Sie keines oder eines der folgenden Authentifizierungsprotokolle: • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) Hinweis Beide Kommunikationspartner müssen das selbe Authentifizierungsverfahren verwenden, ansonsten wird keine Verbindung aufgebaut.

Einstellungen zum ISP-Account

Funktion	Beschreibung
Dauerhafte Verbindung	Ständige Internetverbindung. Nach einer Trennung durch den Provider wird die Verbindung automatisch wieder hergestellt, auch wenn keine Pakete gesendet werden sollen.
On-Demand-Verbindung	Die Internetverbindung wird automatisch aufgebaut, wenn Pakete ins Internet gesendet werden sollen. Werden innerhalb einer bestimmten Zeit keine Pakete gesendet, wird die Internetverbindung automatisch getrennt. Geben Sie im Feld "Maximale Leerlaufzeit" die Minuten ein, nach denen die Verbindung getrennt werden soll. Erlaubte Werte: 10 ... 3600 Verzögerungen beim Versenden der Pakete möglich, wenn Internetverbindung erst aufgebaut werden muss.
Zwangstrennung	Der Provider trennt nach einem bestimmten Zeitraum die Internetverbindung automatisch. Tragen Sie im Feld "Zwangstrennung" eine Uhrzeit ein, trennt das Security-Modul zu diesem Zeitpunkt von sich aus die Internetverbindung. Eine Zwangstrennung in einem ungünstigen Zeitraum wird somit verhindert. Erlaubte Eingaben: 00:00 ... 23:59 Danach erfolgt der Verbindungsaufbau je nach gewählter Verbindungsart: • Dauerhaft: Die Internetverbindung wird sofort wieder aufgebaut. • On-Demand: Die Internetverbindung wird bei Bedarf wieder aufgebaut, z. B. wenn Pakete ins Internet gesendet werden soll.

Einstellungen zur Verbindung

Firewall projektieren

Bedeutung

Die Firewall-Funktionalität der Security-Module hat die Aufgabe, Netze und Stationen vor Fremdbeeinflussungen und Störungen zu schützen. Das bedeutet, dass nur bestimmte, vorher festgelegte Kommunikationsbeziehungen erlaubt werden. Nicht zugelassene Telegramme werden, ohne dass sie eine Antwort senden, von der Firewall verworfen.

Zur Filterung des Datenverkehrs können u. a. IP-Adressen, IP-Subnetze, Portnummern oder MAC-Adressen verwendet werden.

Die Firewall-Funktionalität kann für folgende Protokollebenen konfiguriert werden:

- IP-Firewall mit Stateful Packet Inspection (Layer 3 und 4)
- Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer 2)



Die Firewall kann für den verschlüsselten (IPsec-Tunnel) und den unverschlüsselten Datenverkehr eingesetzt werden.

Firewall-Regeln

Firewall-Regeln beschreiben, welche Pakete in welche Richtung erlaubt bzw. verboten werden.

Automatische Firewall-Regeln für STEP 7-Verbindungen



Für in STEP 7 projektierte Verbindungen werden automatisch Firewall-Regeln in SCT angelegt, die den Kommunikationspartner freigeben. Dabei werden die Aufbaurichtungen der Verbindungen beachtet.

Die Regeln sind nur im Erweiterten Modus sichtbar und könne auch nur dort verändert werden.

Projektierung

Zu unterscheiden sind die beiden Bedienungssichten:

- Im Standard Modus greifen Sie auf einfache, vordefinierte Firewall-Regeln zurück. Sie können nur dienstspezifische Regeln freischalten. Die freigegeben Dienste sind für alle Teilnehmer zulässig und es wird für die angegebene Richtung der volle Zugriff erlaubt.
- Im Erweiterten Modus können Sie detaillierte Firewall-Einstellungen vornehmen. Sie können für einen einzelnen Teilnehmer einzelne Dienste freischalten oder für den Teilnehmer alle Dienste für den Zugriff auf die Station bzw. das Netz freigeben.

Zu unterscheiden sind im Erweiterten Modus die folgenden Firewall-Regelsätze:

- Lokale Firewall-Regeln sind jeweils einem Modul zugewiesen. Sie werden im Eigenschaftsdialog der Module projektiert.
- Globale Firewall-Regeln können mehreren Modulen gleichzeitig zugewiesen werden.
- Benutzerspezifische Firewall-Regeln können mehreren Benutzer und einzelnen Security-Modulen zugewiesen werden.

Zusätzlich haben Sie die Möglichkeit, mit Hilfe von Dienst-Definitionen Firewall-Regeln kompakt und übersichtlich zu definieren. Dienst-Definitionen können sowohl in den lokalen als auch in den globalen Firewall-Regeln eingesetzt werden. Außerdem können Sie eine Bandbreitenbegrenzung einstellen.

Firewall aktivieren

Die Firewall wird im Standard und im Erweiterten Modus durch Aktivieren des Optionskästchen "Firewall aktivieren" gesteuert. Deaktivieren Sie das Kontrollkästchen, werden die Firewall-Regeln, die Sie eingetragen haben, weiterhin in der Liste angezeigt, können jedoch nicht verändert werden. Befindet sich das Security-Modul in einer VPN-Gruppe, ist das Kontrollkästchen standardmäßig aktiviert und kann nicht deaktiviert werden.

Logging-Einstellungen aktivieren

Je nach eingestellter Bedienungssicht unterscheidet sich auch hierfür die Projektierung. Während im Standard Modus das Logging nur für einige vordefinierte Regelsätze pauschal eingeschaltet werden kann, kann es im Erweiterten Modus für jede einzelne Paketfilter-Regel aktiviert werden.

4.1 CPs im Standard Modus

Paketfilter-Regeln aktivieren

Wenn Sie in STEP 7 für die CPs die Security-Funktion aktivieren, sind zunächst alle Zugriffe auf und über den CP zugelassen. Um einzelne Paketfilter-Regeln zu aktivieren, klicken Sie das Kontrollkästchen "Firewall aktivieren". Schalten Sie anschließend die gewünschten Dienste frei. Firewall-Regeln, die aufgrund einer Verbindungsprojektierung automatisch angelegt werden, haben Vorrang vor den hier eingestellten Diensten. Alle anderen Teilnehmer haben vollen Zugriff.

Detaillierte Firewall-Einstellungen im Erweiterten Modus

Im Erweiterten Modus können Sie Firewall-Regeln auf einzelne Teilnehmer beschränken. Um in den Erweiterten Modus zu wechseln, klicken Sie das Optionskästchen "Erweiterter Modus".

Firewall-Projektierung mit VPN

Befindet sich das Security-Modul in einer VPN-Gruppe, ist standardmäßig das Kontrollkästchen "Ausschließlich getunnelte Kommunikation" aktiviert. Dies bedeutet, dass über die externe Schnittstelle keine Kommunikation am Tunnel vorbei gehen darf und nur verschlüsselter IPsec-Datentransfer zugelassen ist. Es wird automatisch die Firewall-Regel "Drop" > "Any" > "Extern" angelegt.

Deaktivieren Sie das Kontrollkästchen, dann sind die getunnelte Kommunikation und zusätzlich die in den anderen Auswahlboxen angewählte Kommunikationsarten zugelassen.

4.1.1 CP x43-1-Advanced

4.1.1.1 Voreinstellung der Firewall

Verhalten mit Voreinstellung

Die folgenden Diagramme zeigen die Standard-Einstellungen im Detail jeweils für den IP-Paketfilter und den MAC-Paketfilter, wenn das Kontrollkästchen "Firewall aktivieren" aktiviert ist und auch im Erweiterten Modus keine Regeln vorhanden sind. Das Verhalten kann durch das Anlegen von entsprechenden Firewall-Regeln im Erweiterten Modus geändert werden.

Standard-Einstellung für CP x43 Adv.

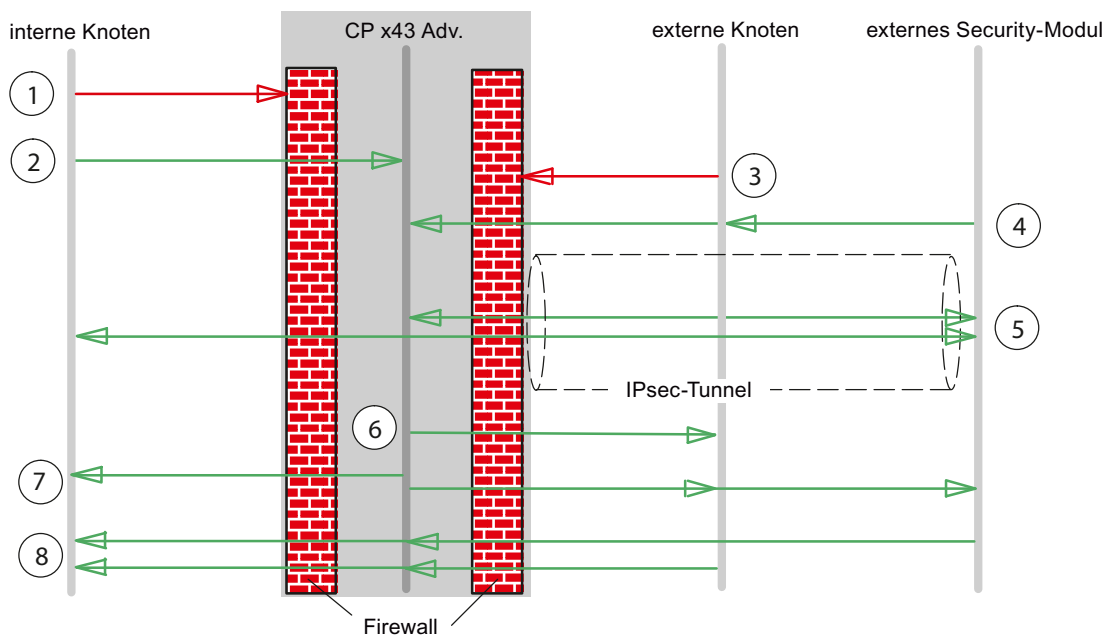


Bild 4-1 Standard-Einstellung für IP-Paketfilter CP x43-1 Adv.

- ① Alle Telegrammtypen von intern nach extern sind geblockt.
 - ② Alle Telegramme von intern an das Security-Modul sind zugelassen.
 - ③ Alle Telegramme von extern nach intern und an das Security-Modul sind geblockt (auch ICMP-Echo-Request).
 - ④ Telegramme von extern (externe Knoten und externe Security-Module) an Security-Modul vom folgenden Typ sind zugelassen:
 - ESP-Protokoll (Verschlüsselung)
 - IKE (Protokoll zum Aufbau der IPsec-Tunnel)
 - NAT-Traversal (Protokoll zum Aufbau der IPsec-Tunnel)
 - ⑤ IP-Kommunikation über IPsec-Tunnel ist zugelassen.
 - ⑥ Telegramme vom Typ Syslog sind vom Security-Modul nach extern zugelassen und werden nicht durch die Firewall beeinflusst.
- Hinweis**
- Da Syslog ein ungesichertes Protokoll ist, kann nicht garantiert werden, dass die Log-Daten gesichert übertragen werden.
- ⑦ Telegramme vom Security-Modul nach intern und extern sind zugelassen.
 - ⑧ Antworten auf Anfragen aus dem internen Netz oder vom Security-Modul sind zugelassen.

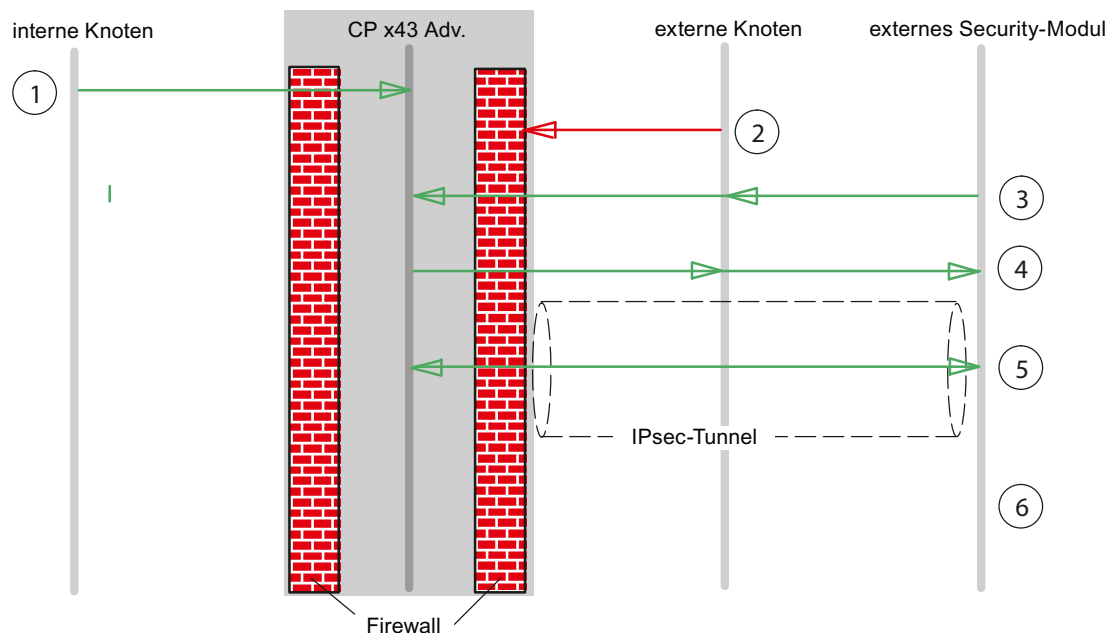


Bild 4-2 Standard-Einstellung für MAC-Paketfilter CP x43-1 Adv.

- ① Alle Telegramme von intern an das Security-Modul sind zugelassen.
- ② Alle Telegramme von extern an das Security-Modul sind geblockt.
- ③ Alle Telegramme von extern an das Security-Modul vom folgenden Typ sind zugelassen:
 - ARP mit Bandbreitenbegrenzung
 - PROFINET-DCP mit Bandbreitenbegrenzung
 - LLDP
- ④ Telegramme vom Security-Modul nach extern vom folgenden Typ sind zugelassen:
 - ARP mit Bandbreitenbegrenzung
 - PROFINET-DCP mit Bandbreitenbegrenzung
- ⑤ Folgende Protokolle, die durch IPsec-Tunnel gesendet werden, sind zugelassen:
 - ISO
 - LLDP

Hinweis

Keine Kommunikation am VPN-Tunnel vorbei

Zusätzlich wird für alle im Projekt bekannten VPN Partnern verhindert, dass eine Kommunikation zwischen den VPN-Endpunkten am Tunnel vorbei möglich ist. Das Verhalten kann auch nicht durch das Anlegen von entsprechenden Firewall-Regeln im Erweiterten Modus geändert werden.

4.1.1.2 Firewall projektieren

So erreichen Sie diese Funktion

1. Markieren Sie das zu bearbeitende Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

Tabelle 4- 1 Verfügbare Dienste und Richtungen

Dienst	Station ⇒ Extern Intern ⇒ Extern	Extern ⇒ Intern	Extern ⇒ Station	Extern ⇔ Station	Freigegebene Ports	Bedeutung
Erlaube IP-Kommunikation	x	x	x	-	-	Der IP-Verkehr für die ausgewählten Kommunikationsrichtungen wird zugelassen.
Erlaube S7-Protokoll	x	x	x	-	TCP Port 102	Kommunikation der Netzwerkteilnehmer über das S7-Protokoll wird zugelassen.
Erlaube FTP/FTPS (expliziter Modus)	x	x	x	-	TCP Port 20 TCP Port 21	Zur Dateiverwaltung und Dateizugriff zwischen Server und Client.
Erlaube HTTP	x	x	x	-	TCP Port 80	Zur Kommunikation mit einem Web-Server.
Erlaube HTTPS	x	x	x	-	TCP Port 443	Zur gesicherten Kommunikation mit einem Web-Server, z. B. zur Web-Diagnose.
Erlaube DNS	x	x	-	-	TCP Port 53 UDP Port 53	Kommunikationsverbindung zu einem DNS-Server wird zugelassen.
Erlaube SNMP	x	x	x	-	TCP Port 161/162 UDP Port 161/162	Zur Überwachung von SNMP-fähigen Netzteilnehmern.
Erlaube SMTP	x	x	-	-	TCP Port 25	Zum Austausch von E-Mails zwischen authentifizierten Benutzern über einen SMTP-Server.
Erlaube NTP	x	x	-	-	UDP Port 123	Zur Synchronisation der Uhrzeit.
Erlaube MAC-Ebene-Kommunikation	-	-	-	x	-	Der MAC-Verkehr von extern zur Station und umgekehrt ist zugelassen.
Erlaube ISO-Kommunikation	-	-	-	x	-	Der ISO-Verkehr von extern zur Station und umgekehrt ist zugelassen.

Tabelle 4- 2 Logging für IP- und MAC-Regelsätze

Regelsatz	Aktion bei Aktivierung	Angelegte Regel		
IP-Log-Einstellungen		Aktion	Von	Nach
Aufzeichnen getunnelter Pakete	Nur aktiv, wenn Security-Modul Teilnehmer einer VPN-Gruppe ist. Alle IP-Pakete die über den Tunnel weitergeleitet wurden, werden geloggt.	Allow	Station	Tunnel
		Allow	Tunnel	Station
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden IP-Pakete die verworfen wurden, werden geloggt.	Drop	Extern	Station
MAC-Log-Einstellungen		Aktion	Von	Nach
Aufzeichnen blockierter eingehender Pakete zur Station	Alle eintreffenden MAC-Pakete die verworfen wurden, werden geloggt.	Drop	Extern	Station
Aufzeichnen blockierter ausgehender Pakete zur Station	Alle ausgehenden MAC-Pakete die verworfen wurden, werden geloggt.	Drop	Station	Extern

Hinweis

Datenverkehr über projektierte Verbindungen wird nicht geloggt.

4.1.1.3 Zugriffsliste projektieren

IP-Zugriffsliste / ACL-Einträge ändern

Die Liste erscheint, wenn in STEP 7 im Register IP-Zugriffsschutz das Optionskästchen "IP-Zugriffsschutz für IP-Kommunikation aktivieren" aktiviert ist.

Über die IP-Zugriffslisten stellen Sie den Zugriffsschutz für bestimmte IP-Adressen ein. Bereits in STEP 7 angelegte Listeneinträge mit den entsprechenden Rechten werden in SCT angezeigt.

Das in STEP 7 auswählbare Recht "Ändern der Accessliste (M)" wird nicht nach SCT übertragen. Damit die zusätzliche IP-Zugriffsberechtigungen übermitteln werden kann, müssen Sie dem entsprechenden Benutzer in SCT das Benutzerecht "Web: IP Access Control-Liste erweitern" zuweisen.

ACHTUNG

Geändertes Verhalten nach Migration

- Nach der Migration wirkt der Zugriffsschutz nur noch an der externen Schnittstelle. Damit der Zugriffsschutz auch an der internen Schnittstelle wirkt, konfigurieren Sie im Erweiterten Modus von SCT die entsprechenden Firewall-Regeln.
- Das Security-Modul antwortet auch auf ARP-Anfragen von nicht freigegebenen IP-Adressen (Layer 2).
- Wenn Sie eine IP Access Control-Liste ohne Einträge migrieren, wird die Firewall aktiviert und auf den CP kann von extern nicht mehr zugegriffen werden. Damit der CP erreichbar ist, konfigurieren Sie im Erweiterten Modus von SCT die entsprechenden Firewall-Regeln.

So erreichen Sie diese Funktion

Menübefehl SCT: Markieren Sie das zu bearbeitende Modul und wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

Menübefehl STEP 7: "IP-Zugriffsschutz" > "Start der Firewall-Konfiguration", Schaltfläche "Ausführen...".

Tabelle 4- 3 Angaben

Parameter	Bedeutung
IP-Adresse	Zugelassene IP-Adresse oder IP-Adressbereich.
Rechte	Je nach getroffener Zuordnung. Rechte, die für die IP-Adresse freigeschaltet sind.
Kommentar	Zusätzliche Kommentareingabe.
Logging	Aktiveren Sie das Kontrollkästchen, werden die Regeln im Paketfilter-Log aufgezeichnet.
Erweiterten Modus aktivieren	Aktiveren Sie das Kontrollkästchen, werden die Einträge in folgende Firewall-Regeln umgewandelt.

Tabelle 4- 4 Schaltflächen

Bezeichnung	Bedeutung / Auswirkung
Neu	Legen Sie eine neue IP-Adresse oder einen neuen IP-Adressbereich mit den dazugehörigen Rechten an.
Ändern	Markieren Sie einen Eintrag und klicken Sie auf diese Schaltfläche, um einen bestehenden Eintrag zu bearbeiten.
Löschen	Löschen Sie über diese Schaltfläche den ausgewählten Eintrag.

4.1.1.4 Eintrag zur Zugriffsliste hinzufügen

Nehmen Sie folgende Einstellungen vor

Feld	Beschreibung
IP-Adresse (oder Start des IP-Bereich)	Geben Sie die IP-Adresse oder den Anfangswert eines IP-Bereichs ein.
Ende des IP-Bereichs (optional)	Geben Sie den Endwert eines IP-Bereichs ein.
Kommentar	Zusätzliche Kommentareingabe; beispielsweise zur Beschreibung des Kommunikationspartners oder des Adressbereiches.
Diese IP-Adresse ist autorisiert für	Zugriff auf Station (A=Access): Kommunikationspartner mit Adressen im angegebenen Bereich haben Zugriff auf die dem CP zugehörige Station (CP / CPU). Diese Zugriffsberechtigung ist für IP-Adressen, die Sie in der Verbindungsprojektierung angegeben haben, implizit gesetzt (gilt nur für spezifizierte Verbindungen). IP-Routing zu anderem Subnetz (R=Routing): Kommunikationspartner mit Adressen im angegebenen Bereich haben Zugriff auf weitere am CP angeschlossene Subnetze. Diese Zugriffsberechtigung ist für IP-Adressen, die Sie in der Verbindungsprojektierung angegeben haben, nicht automatisch gesetzt. Bei Bedarf muss dieses Zugriffsrecht hier explizit gesetzt werden.

Weitere Regeln zur Eingabe:

- Es wird geprüft, ob Einzeladressen mehrfach enthalten sind; hierbei werden erkannt: mehrfache Einzelangabe; Bereichsüberschneidungen.
- Einzeln angegebene IP-Adressen können auch zusätzlich innerhalb eines Bereiches vorkommen; es gelten dann die insgesamt einer IP-Adresse zugewiesenen Zugriffsberechtigungen.
- Es wird nicht geprüft, ob in einem Bereich ungültige Adressen enthalten sind (z. B. können Subnetz-Broadcast-Adressen hier angegeben werden, obwohl sie nicht als IP-Adresse eines Absenders auftreten können).

4.1.2 CP 1628

4.1.2.1 Voreinstellung der Firewall

Verhalten mit Voreinstellung

Die folgenden Diagramme zeigen die Standard-Einstellungen im Detail jeweils für den IP-Paketfilter und den MAC-Paketfilter, wenn das Kontrollkästchen "Firewall aktivieren" aktiviert ist und auch im Erweiterten Modus keine Regeln vorhanden sind. Das Verhalten kann durch das Anlegen von entsprechenden Firewall-Regeln im Erweiterten Modus geändert werden.

Standard-Einstellung für CP 1628

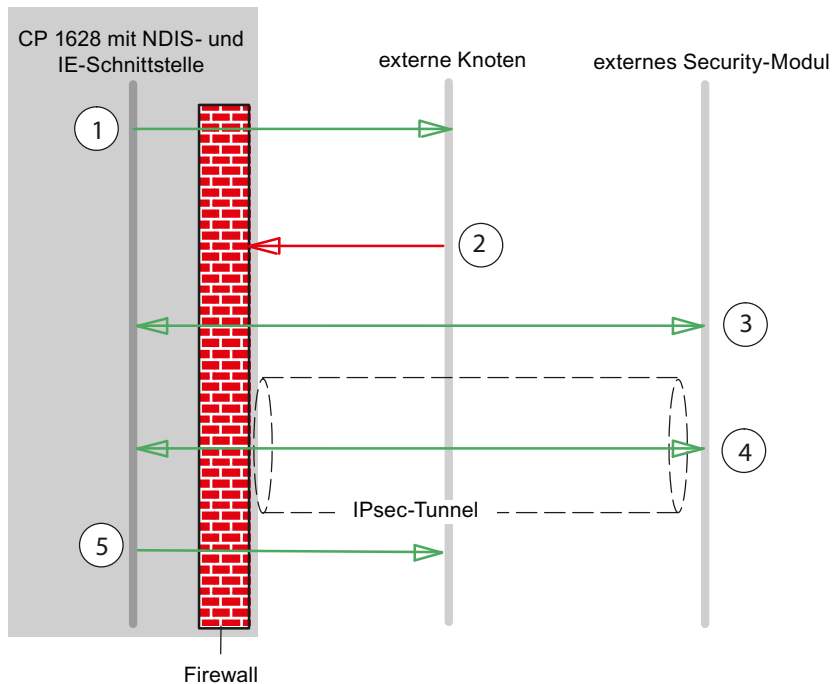


Bild 4-3 Standard-Einstellung für IP-Paketfilter CP 1628

- ① Alle Telegramme von NDIS- und IE (Industrial Ethernet)-Schnittstelle nach extern sind zugelassen.
- ② Alle Telegramme von extern sind geblockt.
- ③ Alle Telegramme von extern an das Security-Modul und umgekehrt vom folgenden Typ sind zugelassen:
 - ESP-Protokoll (Verschlüsselung)
 - IKE (Protokoll zum Aufbau der IPsec-Tunnel)
- ④ IP-Kommunikation über IPsec-Tunnel ist zugelassen.
- ⑤ Telegramme vom Typ Syslog sind vom Security-Modul nach extern zugelassen.

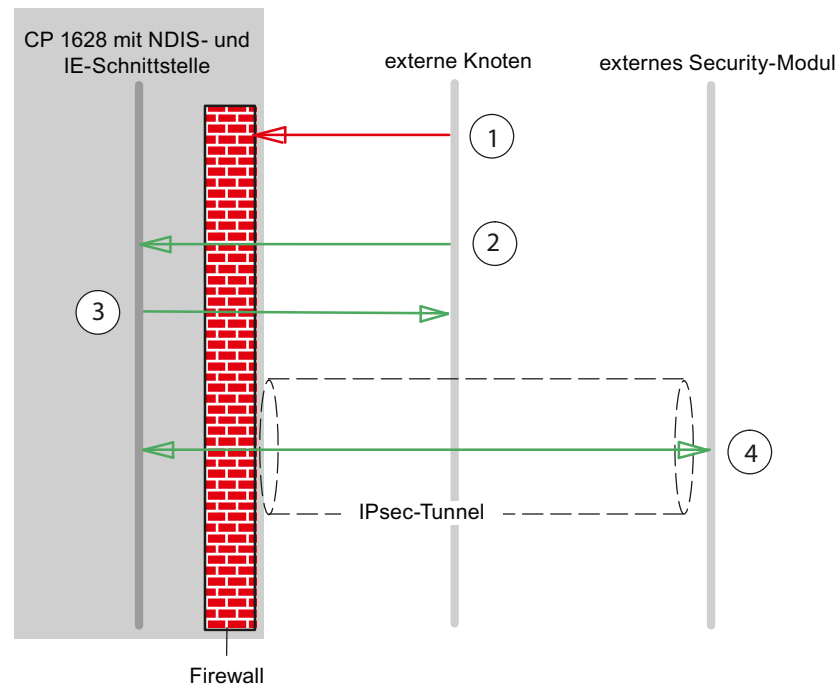


Bild 4-4 Standard-Einstellung für MAC-Paketfilter CP 1628

- ① Alle Telegramme von extern sind geblockt.
- ② Alle Telegramme von extern vom folgenden Typ sind zugelassen:
 - ARP mit Bandbreitenbegrenzung
 - PROFINET-DCP mit Bandbreitenbegrenzung
- ③ Telegramme vom Security-Modul nach extern vom folgenden Typ sind zugelassen:
 - PROFINET-DCP mit Bandbreitenbegrenzung
- ④ MAC-Protokolle, die durch IPsec-Tunnel gesendet werden, sind zugelassen.

Hinweis

Keine Kommunikation am VPN-Tunnel vorbei

Zusätzlich wird für alle im Projekt bekannten VPN Partnern verhindert, dass eine Kommunikation zwischen den VPN-Endpunkten am Tunnel vorbei möglich ist. Das Verhalten kann auch nicht durch das Anlegen von entsprechenden Firewall-Regeln im Erweiterten Modus geändert werden.

4.1.2.2 Firewall projektieren

So erreichen Sie diese Funktion

1. Markieren Sie das zu bearbeitende Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

Tabelle 4- 5 Verfügbare Dienste und Richtungen

Dienst	Extern ⇒ Station	Extern ⇔ Station	Freigegebene Ports	Bedeutung
Erlaube IP-Kommunikation	x	-	-	Der IP-Verkehr für die ausgewählten Kommunikationsrichtungen wird zugelassen.
Erlaube S7-Protokoll	x	-	TCP Port 102	Kommunikation der Netzwerkteilnehmer über das S7-Protokoll wird zugelassen.
Erlaube FTP/FTPS (expliziter Modus)	x	-	TCP Port 20 TCP Port 21	Zur Dateiverwaltung und Dateizugriff zwischen Server und Client.
Erlaube HTTP	x	-	TCP Port 80	Zur Kommunikation mit einem Web-Server.
Erlaube HTTPS	x	-	TCP Port 443	Zur gesicherten Kommunikation mit einem Web-Server, z. B. zur Web-Diagnose.
Erlaube DNS	x	-	TCP Port 53 UDP Port 53	Kommunikationsverbindung zu einem DNS-Server wird zugelassen.
Erlaube SNMP	x	-	TCP Port 161/162 UDP Port 161/162	Zur Überwachung von SNMP-fähigen Netzteilnehmern.
Erlaube SMTP	x	-	TCP Port 25	Zum Austausch von E-Mails zwischen authentifizierten Benutzern über einen SMTP-Server.
Erlaube NTP	x	-	UDP Port 123	Zur Synchronisation der Uhrzeit.
Erlaube MAC-Ebene-Kommunikation	-	x	-	Der MAC-Verkehr von extern zur Station und umgekehrt ist zugelassen.
Erlaube ISO-Kommunikation	-	x	-	Der ISO-Verkehr von extern zur Station und umgekehrt ist zugelassen.
Erlaube SiClock	-	x	-	SiClock-Uhrzeittelegramme von extern zur Station und umgekehrt sind zugelassen.

Tabelle 4- 6 Logging für IP- und MAC-Regelsätze

Regelsatz	Aktion bei Aktivierung	Angelegte Regel		
IP-Log-Einstellungen		Aktion	Von	Nach
Aufzeichnen getunnelter Pakete	Nur aktiv, wenn Security-Modul Teilnehmer einer VPN-Gruppe ist. Alle IP-Pakete die über den Tunnel weitergeleitet wurden, werden geloggt.	Allow	Station	Tunnel
		Allow	Tunnel	Station
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden IP-Pakete die verworfen wurden, werden geloggt.	Drop	Extern	Station
MAC-Log-Einstellungen		Aktion	Von	Nach
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden MAC-Pakete die verworfen wurden, werden geloggt.	Drop	Extern	Station
Aufzeichnen blockierter ausgehender Pakete	Alle ausgehenden MAC-Pakete die verworfen wurden, werden geloggt.	Drop	Station	Extern

Hinweis

Datenverkehr über projektierte Verbindungen wird nicht geloggt.

4.2 SCALANCE S im Standard Modus

4.2.1 Voreinstellung der Firewall

Verhalten mit Voreinstellung

Die folgenden Diagramme zeigen die Standard-Einstellungen im Detail jeweils für den IP-Paketfilter und den MAC-Paketfilter. Das Verhalten kann durch das Anlegen von entsprechenden Firewall-Regeln im Erweiterten Modus geändert werden.

Standard-Einstellung für SCALANCE S

Die Voreinstellung für die Firewall ist so gewählt, dass kein IP-Datenverkehr möglich ist. Lediglich über ggf. konfigurierte IPsec-Tunnel ist Kommunikation zwischen den Knoten in den internen Netzen von Security-Modulen zugelassen.

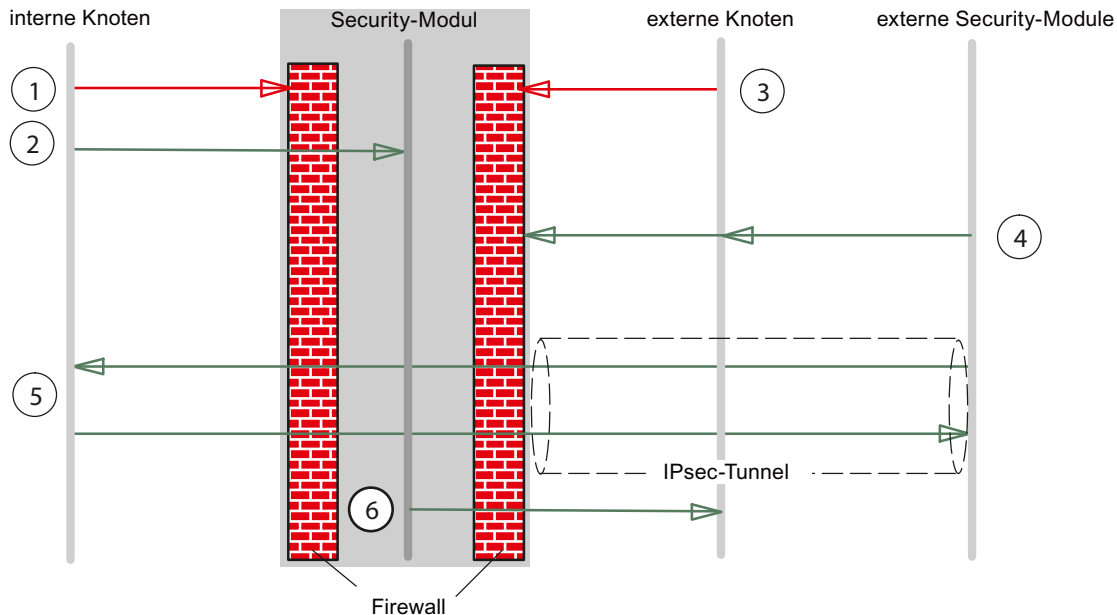


Bild 4-5 Standard-Einstellung für IP-Paketfilter SCALANCE S

- ① Alle Telegrammtypen von intern nach extern sind geblockt.
- ② Alle Telegramme von intern an das Security-Modul sind zugelassen.
- ③ Alle Telegramme von extern nach intern und an das Security-Modul sind geblockt (auch ICMP-Echo-Request).
- ④ Telegramme von extern (externe Knoten und externe Security-Module) an Security-Module vom folgenden Typ sind zugelassen:
 - HTTPS (SSL)
 - ESP-Protokoll (Verschlüsselung)
 - IKE (Protokoll zum Aufbau der IPsec-Tunnel)
 - NAT-Traversal (Protokoll zum Aufbau der IPsec-Tunnel)
- ⑤ IP-Kommunikation über IPsec-Tunnel ist zugelassen.
- ⑥ Telegramme vom Typ Syslog und NTP sind vom Security-Modul nach extern zugelassen.

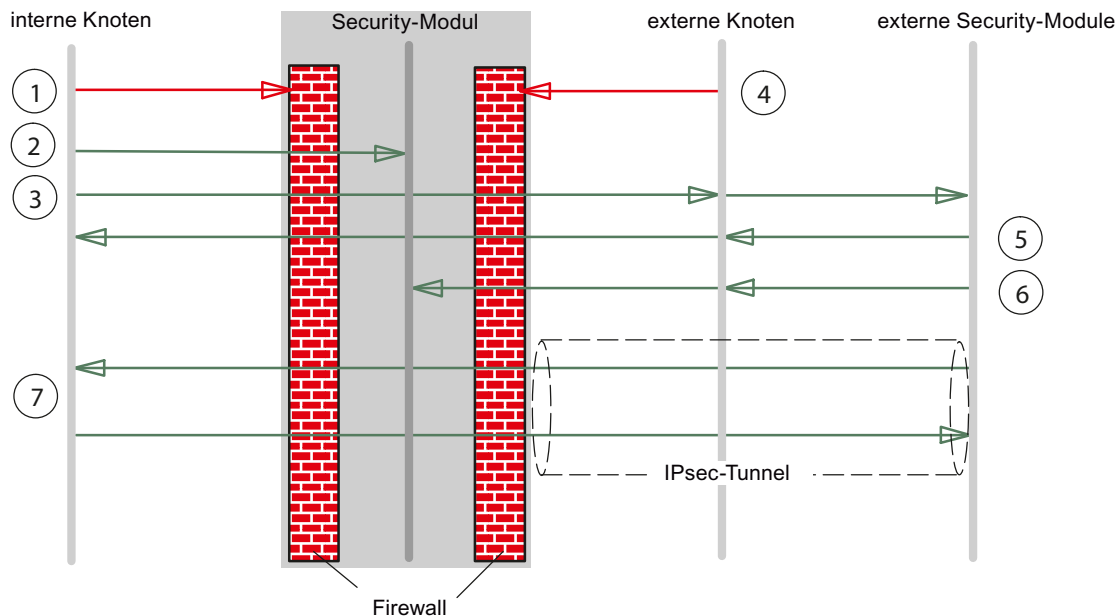


Bild 4-6 Standard-Einstellung für MAC- Paketfilter SCALANCE S

- ① Alle Telegrammtypen von intern nach extern sind geblockt.
- ② Alle Telegramme von intern an das Security-Modul sind zugelassen.
- ③ ARP-Telegramme von intern nach extern sind zugelassen.
- ④ Alle Telegramme von extern nach intern und an das Security-Modul sind geblockt.
- ⑤ Telegramme von extern nach intern von folgendem Typ sind zugelassen:
 - ARP mit Bandbreitenbegrenzung
- ⑥ Telegramme von extern an Security-Module vom folgenden Typ sind zugelassen:
 - ARP mit Bandbreitenbegrenzung
 - PROFINET-DCP mit Bandbreitenbegrenzung
- ⑦ MAC-Protokolle, die durch IPsec-Tunnel gesendet werden, sind zugelassen.

4.2.2 Firewall projektieren ≥ V3.0

So erreichen Sie diese Funktion

1. Markieren Sie das zu bearbeitende Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

Firewall standardmäßig aktiviert

Das Kontrollkästchen "Firewall aktivieren" ist standardmäßig aktiviert. Die Firewall ist also automatisch aktiviert und alle Zugriffe von extern auf das Security-Modul sind gesperrt. Schalten Sie durch Anklicken der entsprechenden Kontrollkästchen die Firewall-Regeln für die jeweiligen Richtungen frei.

Detaillierte Firewall-Einstellungen im Erweiterten Modus

Im Erweiterten Modus können Sie Firewall-Regeln auf einzelne Teilnehmer beschränken.

Firewall-Projektierung mit VPN

Befindet sich das Security-Modul in einer VPN-Gruppe, ist standardmäßig das Kontrollkästchen "Ausschließlich getunnelte Kommunikation" aktiviert. Dies bedeutet, dass über die externe Schnittstelle keine Kommunikation am Tunnel vorbei gehen darf und nur verschlüsselter IPsec-Datentransfer zugelassen ist.

Deaktivieren Sie das Kontrollkästchen, dann sind die getunnelte Kommunikation und zusätzlich die in den anderen Auswahlboxen angewählten Kommunikationsarten zugelassen.

Tabelle 4- 7 Verfügbare Firewall-Regeln und Richtungen

Dienst	Intern ⇒ Extern	Extern ⇒ Intern	Von Intern	Von Extern	Freigegebene Ports	Bedeutung
Erlaube IP-Verkehr	x	x	-	-	-	Der IP-Verkehr für die ausgewählten Kommunikationsrichtungen wird zugelassen.
Erlaube S7-Protokoll	x	x	-	-	TCP Port 102	Kommunikation der Netzwerkteilnehmer über das S7-Protokoll wird zugelassen.
Erlaube FTP/FTPS (expliziter Modus)	x	x	-	-	TCP Port 20 TCP Port 21	Zur Dateiverwaltung und Dateizugriff zwischen Server und Client.
Erlaube HTTP	x	x	-	-	TCP Port 80	Zur Kommunikation mit einem Web-Server.
Erlaube HTTPS	x	x	-	-	TCP Port 443	Zur gesicherten Kommunikation mit einem Web-Server, z. B. zur Web-Diagnose.
Erlaube mit DNS	x	x	-	-	TCP Port 53 UDP Port 53	Kommunikationsverbindung zu einem DNS-Server wird zugelassen.

Dienst	Intern → Extern	Extern → Intern	Von Intern	Von Extern	Freigegebene Ports	Bedeutung
Erlaube mit SNMP	x	x	-	-	TCP Port 161/162 UDP Port 161/162	Zur Überwachung von SNMP-fähigen Netzteilnehmern.
Erlaube mit SMTP	x	x	-	-	TCP Port 25	Zum Austausch von E-Mails zwischen authentifizierten Benutzern über einen SMTP-Server.
Erlaube NTP	x	x	-	-	UDP Port 123	Zur Synchronisation der Uhrzeit.
Erlaube DHCP	x	x	-	-		
Erlaube MAC-Ebene-Kommunikation	-	-	x	x	-	Der MAC-Verkehr von extern zur Station und umgekehrt ist zugelassen.
Erlaube ISO-Protokoll	-	-	x	x	-	Der ISO-Verkehr von extern zur Station und umgekehrt ist zugelassen.
Erlaube SiClock	-	-	x	x	-	SiClock-Uhrzeittelegramme von extern zur Station und umgekehrt sind zugelassen.
Erlaube DCP	-	-	x	x	-	

Tabelle 4- 8 Logging für IP- und MAC-Regelsätze

Regelsatz	Aktion bei Aktivierung
IP-Log-Einstellungen	
Aufzeichnen getunnelter Pakete	Nur aktiv, wenn Security-Modul Teilnehmer einer VPN-Gruppe ist. Alle IP-Pakete die über den Tunnel weitergeleitet wurden, werden geloggt.
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden IP-Pakete die verworfen wurden, werden geloggt.
Aufzeichnen blockierter ausgehender Pakete	Alle ausgehenden IP-Pakete die verworfen wurden, werden geloggt.
MAC-Log-Einstellungen	
Aufzeichnen getunnelter Pakete	Nur aktiv, wenn Security-Modul Teilnehmer einer VPN-Gruppe ist. Alle MAC-Pakete die über den Tunnel weitergeleitet wurden, werden geloggt.
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden MAC-Pakete die verworfen wurden, werden geloggt.
Aufzeichnen blockierter ausgehender Pakete	Alle ausgehenden MAC-Pakete die verworfen wurden, werden geloggt.

4.2.3 Firewall projektieren < V3.0

So erreichen Sie diese Funktion

1. Markieren Sie das zu bearbeitende Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

Hinweis

Detaillierte Firewall-Einstellungen im Erweiterten Modus

Im Erweiterten Modus können Sie Firewall-Regeln auf einzelne Teilnehmer beschränken. Um in den Erweiterten Modus zu wechseln, klicken Sie das Optionskästchen "Erweiterter Modus aktivieren".

Tabelle 4- 9 Verfügbare Dienste und Richtungen

Regel / Option	Freigegebene Ports	Funktion
Ausschließlich getunnelte Kommunikation	-	Das ist die Standardeinstellung. Die Option ist nur dann wählbar, wenn sich das Modul in einer Gruppe befindet. Mit dieser Einstellung wird nur verschlüsselter IPsec-Datentransfer zugelassen; nur Knoten in internen Netzen von SCALANCE S können miteinander kommunizieren. Wenn diese Option abgewählt ist, dann ist die getunnelte Kommunikation und zusätzlich die in den anderen Auswahlboxen angewählte Kommunikationsart zugelassen.
Erlaube IP-Verkehr vom internen ins externe Netz	-	Interne Knoten können eine Kommunikationsverbindung zu Knoten im externen Netz initiieren. Nur Antworttelegramme aus dem externen Netz werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.
Erlaube IP-Verkehr mit S7-Protokoll vom internen ins externe Netz.	TCP Port 102	Interne Knoten können eine S7-Kommunikationsverbindung zu Knoten im externen Netz initiieren. Nur Antworttelegramme aus dem externen Netz werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.
Erlaube Zugriff auf DHCP-Server vom internen ins externe Netz.	UDP Port 67 UDP Port 68	Interne Knoten können eine Kommunikationsverbindung zu einem DHCP-Server im externen Netz initiieren. Nur die Antworttelegramme des DHCP-Servers werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.
Erlaube Zugriff auf NTP-Server vom internen ins externe Netz.	UDP Port 123	Interne Knoten können eine Kommunikationsverbindung zu einem NTP-Server (Network Time Protocol) im externen Netz initiieren. Nur die Antworttelegramme des NTP-Servers werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.

Regel / Option	Freigegebene Ports	Funktion
Erlaube SiClock-Uhrzeitlegramme vom externen ins interne Netz.	-	Mit dieser Option werden SiClock-Uhrzeitlegramme vom externen ins interne Netz freigegeben.
Erlaube Zugriff auf DNS-Server vom internen ins externe Netz.	TCP Port 53 UDP Port 53	Interne Knoten können eine Kommunikationsverbindung zu einem DNS-Server im externen Netz initiieren. Nur die Antworttelegramme des DNS-Servers werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.
Erlaube die Konfiguration von internen Netzknoten mittels DCP vom externen ins interne Netz.	-	Das DCP-Protokoll wird vom PST-Tool verwendet, um bei SIMATIC Net Netzkomponenten die Knotentaufe (Einstellen der IP-Parameter) vorzunehmen. Mit dieser Regel wird Knoten im externen Netz erlaubt, per DCP-Protokoll auf Knoten im internen Netz zuzugreifen.

Tabelle 4- 10 Logging für IP- und MAC-Regelsätze

Regelsatz	Aktion bei Aktivierung
IP-Log-Einstellungen	
Aufzeichnen getunnelter Pakete	Nur wenn Security-Modul Teilnehmer einer VPN-Gruppe: Alle IP-Pakete die über den Tunnel weitergeleitet wurden, werden geloggt.
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden IP-Pakete die verworfen wurden, werden geloggt.
Aufzeichnen blockierter ausgehender Pakete	Alle ausgehenden IP-Pakete die verworfen wurden, werden geloggt.
MAC-Log-Einstellungen	
Aufzeichnen blockierter eingehender Pakete	Alle eintreffenden MAC-Pakete die verworfen wurden, werden geloggt.
Aufzeichnen blockierter ausgehender Pakete	Alle ausgehenden MAC-Pakete die verworfen wurden, werden geloggt.

4.3 Im Erweiterten Modus

Im Erweiterten Modus gibt es erweiterte Einstellmöglichkeiten, die eine individuelle Einstellung der Firewall-Regeln und der Sicherheitsfunktionalität zulassen.

In den Erweiterten Modus umschalten

Schalten Sie für alle in diesem Kapitel beschriebenen Funktionen in den Erweiterten Modus um.

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.

Abhilfe SCT Standalone: Sie schließen das Projekt ohne zu speichern und öffnen es erneut.

Symbolische Namen werden unterstützt

Sie können in den nachfolgend beschriebenen Funktionen IP-Adressen oder MAC-Adressen auch als symbolische Namen eingeben.

4.3.1 Firewall projektieren

Im Gegensatz zur Projektierung fest vorgegebener Paketfilter-Regeln im Standard Modus können Sie im Erweiterten Modus von Security Configuration Tool individuelle Paketfilter-Regeln projektieren.

Die Paketfilter-Regeln stellen Sie in wählbaren Registern für folgende Protokolle ein:

- IP-Protokoll (Schicht/Layer 3)
- MAC-Protokoll (Schicht/Layer 2)

Hinweis

Keine MAC-Regeln bei aktiviertem Routing-Modus

SCA.

Wenn Sie für das Security-Modul den Routing-Modus aktiviert haben, finden MAC-Regeln keine Anwendung (Dialoge sind inaktiv).

Wenn Sie in den nachfolgend beschriebenen Dialogen keine Regel eintragen, gelten die Standardeinstellungen entsprechend der Beschreibung in den jeweiligen Unterkapiteln des Kapitels CPs im Standard Modus (Seite 88).

Globale, benutzerspezifische und lokale Definition möglich

- Globale Firewall-Regeln

Eine globale Firewall-Regel kann mehreren Modulen gleichzeitig zugewiesen werden. Diese Möglichkeit vereinfacht in vielen Fällen die Projektierung.

- Benutzerspezifische Firewall-Regeln S≥V3.0

Eine benutzerspezifische Firewall-Regel kann einem oder mehreren Benutzern und anschließend einzelnen Security-Modulen zugewiesen werden.

- Lokale Firewall-Regeln

Eine lokale Firewall-Regel ist jeweils einem Modul zugewiesen. Sie wird im Eigenschaftendialog eines Moduls projiziert.

Einem Modul können mehrere lokale Firewall-Regeln, mehrere globale Firewall-Regeln und mehrere benutzerdefinierte Firewall-Regeln zugewiesen werden.

4.3.2 Globale Firewall-Regeln

Anwendung

Globale Firewall-Regeln werden außerhalb der Module auf Projektebene projiziert. Sie sind im Navigationsbereich des Security Configuration Tool sichtbar.

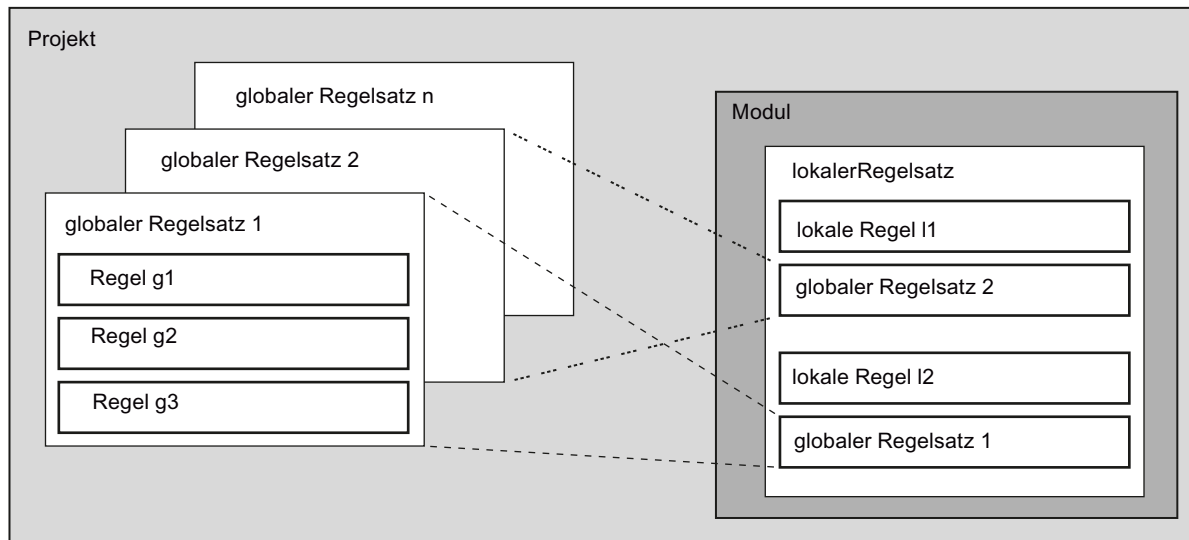
Unterschieden wird bei den globalen Firewall-Regeln zwischen:

- IP-Firewall-Regeln
- MAC-Firewall-Regeln

Globale Firewall-Regeln können definiert werden für:

- IP-Regelsätze
- MAC-Regelsätze

Die folgende Darstellung verdeutlicht den Zusammenhang zwischen global definierten Regelsätzen und lokal verwendeten Regelsätzen.



Wann sind globale IP- und MAC-Firewall-Regeln sinnvoll?

Globale Firewall-Regeln sind dann sinnvoll, wenn Sie für mehrere Security-Module identische Filterkriterien für die Kommunikation definieren wollen.

Hinweis

Nur Regelsätze zuweisen, die vom Security-Modul unterstützt werden

Eine fehlerhafte Modulzuordnung kann zu unerwünschten Ergebnissen führen. Überprüfen Sie daher immer die modulspezifischen lokalen Firewall-Regeln im Ergebnis. Eine falsche Regelzuordnung wird bei der automatischen Konsistenzprüfung nicht erkannt. Es werden nur die Regeln übernommen, die das Security-Modul auch unterstützt.

Siehe auch

Benutzerspezifische Firewall-Regeln (Seite 110)

4.3.2.1 Globale Firewall-Regelsätze - Vereinbarungen

Globale Firewall-Regeln werden lokal genutzt

Folgende Vereinbarungen gelten bei der Erstellung eines globalen Firewall-Regelsatzes sowie bei der Zuweisung zu einem Modul:

- Ansicht im Security Configuration Tool
Globale Firewall-Regeln können nur im Erweiterten Modus angelegt werden.
- Priorität
Globale IP- und MAC-Firewall-Regeln: Lokal definierte Regeln haben standardmäßig eine höhere Priorität als globale IP- und MAC-Firewall-Regeln; neu zugewiesene globale IP- und MAC-Firewall-Regeln werden daher in der lokalen Regelliste zunächst unten eingefügt.
Die Priorität kann durch Verändern der Platzierung in der Regelliste verändert werden.
- Granularität
Globale Firewall-Regeln können nur als ganzer Regelsatz einem Security-Modul zugeordnet werden.
- Regelsätze eingeben, ändern oder löschen
Globale Firewall-Regeln sind in der lokalen Regelliste der Firewall-Regeln bei den Moduleigenschaften nicht editierbar. Sie können dort nur angezeigt und gemäß der gewünschten Priorität platziert werden.
Eine einzelne Regel kann nicht aus einem zugeordneten Regelsatz gelöscht werden. Es kann nur der komplette Regelsatz aus der lokalen Regelliste genommen werden; die Definition in der globalen Regelliste wird dadurch nicht verändert.

4.3.2.2 Globale Firewall-Regelsätze einstellen und zuweisen

So erreichen Sie diese Funktion

1. Wählen Sie im Navigationsbereich einen der folgenden Ordner:
 - "Globale FW-Regelsätze" > "FW IP-Regelsätze"
 - "Globale FW-Regelsätze" > "FW MAC-Regelsätze"
2. Wählen Sie den Menübefehl "Einfügen" > "Firewall Regelsatz".
3. Geben Sie die folgenden Daten ein:
 - Name: Projektweit eindeutige Bezeichnung des Regelsatzes; der Name erscheint nach der Zuweisung des Regelsatzes in der lokalen Regelliste des Security-Moduls.
 - Beschreibung: Geben Sie eine Beschreibung für den globalen Regelsatz ein.
4. Klicken Sie auf die Schaltfläche "Regel hinzufügen".

5. Tragen Sie der Reihe nach die Firewall-Regeln in die Liste ein. Beachten Sie die Parameterbeschreibung in folgenden Kapiteln:
Für IP-Regelsätze: IP-Paketfilter-Regeln (Seite 116).
Für MAC-Regelsätze: MAC-Paketfilter-Regeln (Seite 125).
6. Ordnen Sie die globale Firewall-Regel den Modulen zu, in denen diese verwendet werden soll. Markieren Sie dazu im Navigationsbereich ein Modul und ziehen Sie dieses auf den passenden globalen Regelsatz im Navigationsbereich (Drag and Drop).

Ergebnis

Der globale Regelsatz wird vom zugewiesenen Security-Modul als lokaler Regelsatz verwendet und erscheint automatisch in der modulspezifischen Liste der Firewall-Regeln.

Siehe auch

Globale Firewall-Regelsätze - Vereinbarungen (Seite 109)

4.3.3 Benutzerspezifische Firewall-Regeln

S≥V3.0

Wann ist die Zuordnung von IP-Firewall-Regeln zu einem Benutzer sinnvoll?

IP-Firewall-Regeln werden zunächst einem oder mehreren Benutzern und anschließend einzelnen Security-Modulen zugeordnet. Dadurch ist es möglich, benutzerspezifische Zugriffe zu erlauben. Wenn z. B. standardmäßig alle Zugriffe auf die Netze hinter einem Security-Modul gesperrt sind, können bestimmte IP-Adressen für einen Benutzer freigeschaltet werden. Somit ist für diesen Benutzer der Zugriff erlaubt, für andere Benutzer bleiben die Zugriffe weiterhin gesperrt.

Anmelden des Benutzers über das Internet

Der Benutzer kann sich über eine Webseite am Security-Modul anmelden. Wenn die Authentifizierung erfolgreich ist, wird der für diesen Benutzer vordefinierte Firewall-Regelsatz aktiviert. Die Verbindung zum Security-Modul erfolgt dabei über HTTPS unter Verwendung der IP-Adresse des angebundenen Ports bei Beachtung der gültigen Routing-Regeln:

Beispiel:

Externer Port: 192.168.10.1

Anmeldung über: <https://192.168.10.1/>

Anmelden können sich Benutzer mit der Rolle administrator, diagnostics oder remote access, sofern diese einer benutzerspezifischen Firewall-Regel zugeordnet ist.

Benutzerspezifische Firewall-Regeln werden lokal genutzt - Vereinbarungen

Es gelten die selben Vereinbarungen wie im Kapitel Globale Firewall-Regelsätze - Vereinbarungen (Seite 109).

4.3.3.1 Benutzerspezifische Firewall-Regeln einstellen und zuweisen

So erreichen Sie diese Funktion

1. Wählen Sie im Navigationsbereich den Ordner "Benutzerspez. IP-Regelsätze".
2. Wählen Sie den Menübefehl "Einfügen" > "Firewall Regelsatz".
3. Geben Sie die folgenden Daten ein:
 - Name: Projektweit eindeutige Bezeichnung des Regelsatzes; der Name erscheint nach der Zuweisung des Regelsatzes in der lokalen Regelliste des Security-Moduls.
 - Beschreibung: Geben Sie eine Beschreibung für den benutzerdefinierten Regelsatz ein.
4. Klicken Sie auf die Schaltfläche "Regel hinzufügen".
5. Tragen Sie der Reihe nach die Firewall-Regeln in die Liste ein. Beachten Sie die Parameterbeschreibung im Kapitel IP-Paketfilter-Regeln (Seite 116).
6. Weisen Sie die Regel einem oder mehreren Benutzern zu.

Hinweis

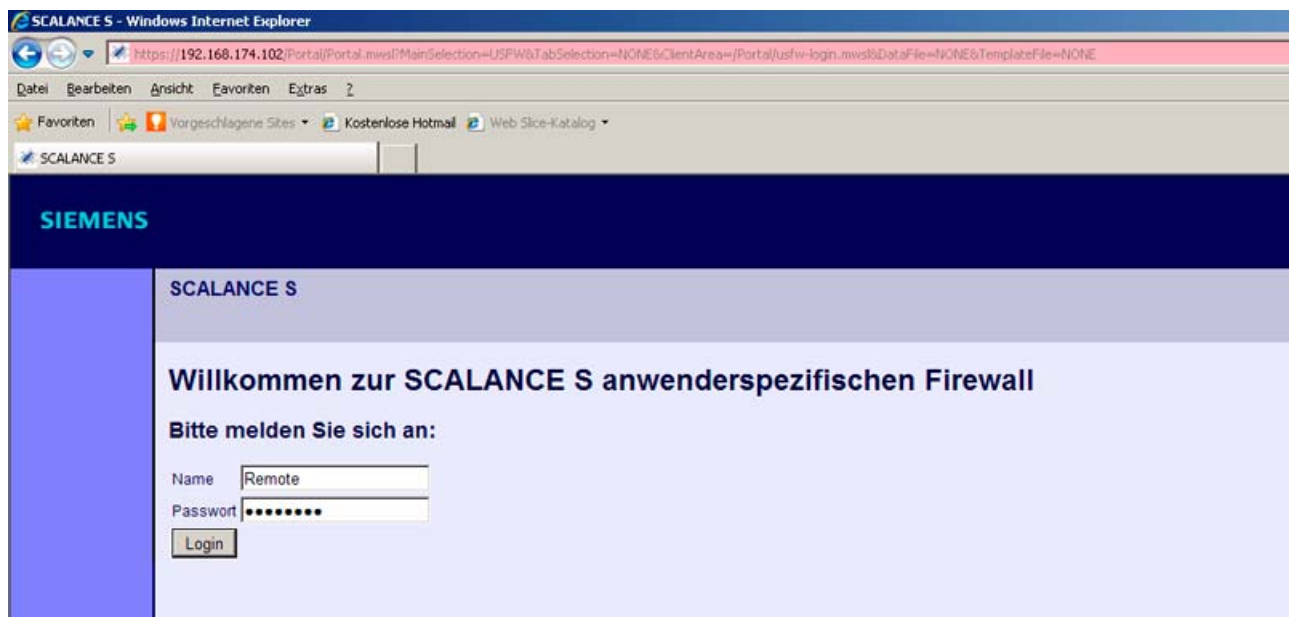
Zuordnung von benutzerspezifischen Regelsätzen

- Einer Baugruppe kann nur ein benutzerspezifischer Regelsatz pro Benutzer zugewiesen werden.
 - Durch die Zuordnung wird für alle Rollen der im Regelsatz festgelegten Benutzer das Recht "Benutzer darf sich an Baugruppe anmelden" aktiviert.
-

7. Ordnen Sie die benutzerspezifische Firewall-Regel den Security-Modulen zu, in denen sie verwendet werden soll. Wählen Sie dazu im Navigationsbereich ein Modul und ziehen Sie dieses auf den passenden benutzerspezifischen Regelsatz im Navigationsbereich (Drag and Drop).

Ergebnis

- Der benutzerspezifische Regelsatz wird vom zugewiesenen Security-Modul als lokaler Regelsatz verwendet und erscheint automatisch in der modulspezifischen Liste der Firewall-Regeln.
- Der Benutzer kann sich am Security-Modul anmelden.



Wertebereiche für Timeout

Die Timeout-Zeit, nach deren Ablauf der Benutzer automatisch abgemeldet wird, beträgt 30 Minuten.

4.3.4 Verbindungsbezogene automatische Firewall-Regeln



Automatisch angelegte Firewall-Regeln in SCT

Für folgenden Anwendungsfall werden automatisch Firewall-Regeln angelegt:

- In STEP 7 projektierte Verbindungen

Firewall-Regeln für projektierte Verbindungen

Sind in STEP 7 Verbindungen angelegt, werden für diese in SCT automatisch Firewall-Regeln erstellt. Dazu findet ein Systemabgleich zwischen STEP 7 und SCT statt, bei dem alle projektierten Verbindungen im Projekt überprüft werden. Automatisch abgeglichen werden für jeden Kommunikationspartner die IP-Adresse, die Aktion und die Schnittstelle. Pro Kommunikationspartner entstehen unabhängig von der Anzahl der Verbindungen 2 Regeln.

Hinweis

UDP-Multicast- und UDP-Broadcast-Verbindungen manuell freigeben

S7-CP

Für UDP-Multicast- und UDP-Broadcast-Verbindungen werden keine automatischen Firewall-Regeln angelegt. Um die Verbindungen freizugeben, fügen Sie die entsprechenden Firewall-Regeln im Erweiterten Modus manuell hinzu.

Je nachdem, wie in STEP 7 der Verbindungsaufbau projektiert ist, werden in SCT die folgenden Ebene 3-Firewall-Regeln angelegt:

CP->extern	Aktion	Von	Nach
aktiv	Allow	Station	Extern
	Drop	Extern	Station
passiv	Drop	Station	Extern
	Allow	Extern	Station
aktiv und passiv	Allow	Extern	Station
	Allow	Station	Extern

Befindet sich das Security-Modul in einer VPN-Gruppe, wechselt die Richtung "Extern" in "Tunnel".

CP->intern	Aktion	Von	Nach
aktiv	Allow	Station	Intern
	Drop	Intern	Station
passiv	Drop	Station	Intern
	Allow	Intern	Station
aktiv und passiv	Allow	Intern	Station
	Allow	Station	Intern

Für Ebene 2-Verbindungen werden nur "Allow"-Regeln angelegt.

Vereinbarungen für automatisch angelegte Firewall-Regeln

- **Priorität**
Die Regeln haben die höchste Priorität und werden daher in der lokalen Regelliste oben eingefügt.
- **Regeln ändern oder löschen**
Die Regelsätze können nicht gelöscht werden. Das Logging kann aktiviert und Dienste können zugewiesen werden. Außerdem kann die Bandbreite und ein Kommentar eingefügt werden.
- **Aktion umstellen**
Stellen Sie in SCT die Aktion von "Allow" auf "Drop" oder umgekehrt um, werden diese beim erneuten Systemabgleich wieder überschrieben. Soll die vorgenommene Änderungen bestehen bleiben, wählen Sie als Aktion "Allow*" oder "Drop*". In diesem Fall wird nur die IP-Adresse mit STEP 7 abgeglichen und Aktion und Richtung bleiben wie eingestellt bestehen. Ist die IP-Adresse in STEP 7 nicht vorhanden, wird die Regel aus der Liste entfernt. Einstellungen zu Logging, Dienst, Bandbreite und Kommentar in SCT bleiben auch bei einem erneuten Systemabgleich mit STEP 7 bestehen.

Security-Modul in VPN-Gruppe

Standardmäßig wird das Kontrollkästchen "Ausschließlich getunnelte Kommunikation" aktiviert. Deaktivieren Sie das Kontrollkästchen, kann die Kommunikation durch oder am Tunnel vorbei laufen.

- Die Kommunikation läuft außerhalb des Tunnels, wenn die Partneradresse zu einer im SCT bekannten Station gehört, zu der kein VPN-Tunnel projiziert ist.
- Die Kommunikation läuft durch den VPN-Tunnel, wenn die Partneradresse ein VPN-Endpunkt ist.
- Kann nicht eindeutig zugeordnet werden, ob eine Verbindung innerhalb oder außerhalb des VPN-Tunnels laufen soll, wird die Verbindung dem VPN-Tunnel zugeordnet und ein entsprechender Hinweis wird angezeigt. Die Zuordnung kann im Erweiterten Modus, z. B. durch Ändern der "Von"-Richtung "Tunnel" auf "Extern", angepasst werden,

Hinweis

Soll sichergestellt werden, dass ausschließlich eine Kommunikation durch den Tunnel möglich ist, müssen Sie im Erweiterten Modus entsprechende Firewall-Regeln, z. B für interne Teilnehmer oder NDIS-Adressen, anlegen.

Um für einen CP ausschließlich getunnelte Kommunikation zuzulassen, fügen Sie am Ende der Firewall-Regeln eine Regel "Drop" > "Any" > "Station" ein.

4.3.5 Lokale IP-Paketfilter-Regeln einstellen

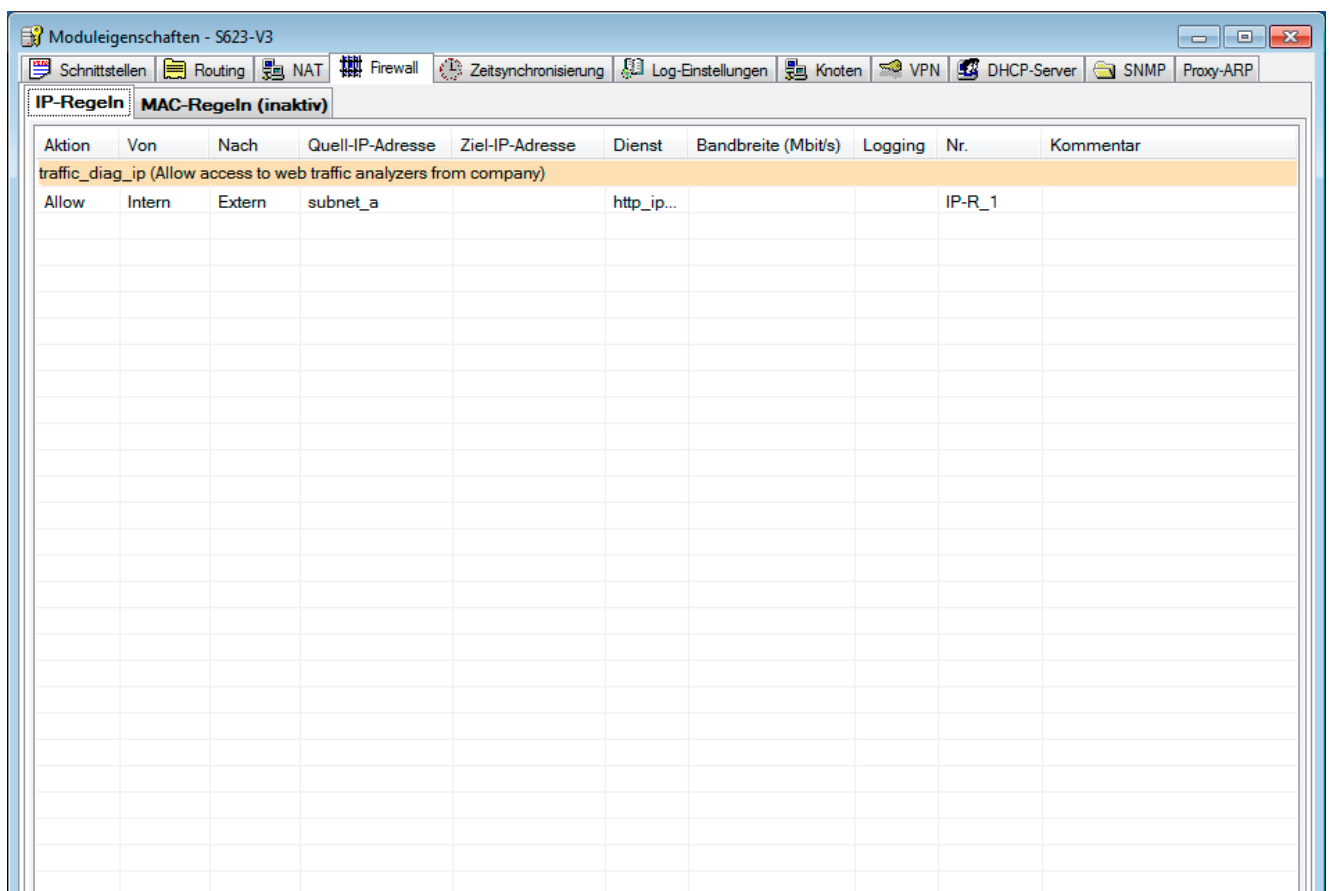
Mittels IP-Paketfilter-Regeln können Sie auf IP-Telegramme wie beispielsweise UDP-, TCP-, ICMP-Telegramme filtern.

Innerhalb einer IP-Paketfilter-Regel können Sie auf Dienst-Definitionen zurückgreifen und damit die Filterkriterien weiter eingrenzen. Wenn Sie keine Dienste angeben, gilt die IP-Paketfilter-Regel für alle Dienste.

Dialog für lokale IP-Paketfilter-Regeln öffnen

SCT: Markieren Sie das zu bearbeitende Modul und wählen den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall".

STEP 7: Klicken Sie im Register "Security" neben "Start der Security-Konfiguration" auf die Schaltfläche "Ausführen", Register "Firewall".



IP-Paketfilter-Regeln eintragen

Tragen Sie der Reihe nach die Firewall-Regeln in die Liste ein; beachten Sie die Parameterbeschreibung und die Beispiele im Folgekapitel oder in der Online-Hilfe.

Globale und benutzerspezifische Regelsätze nutzen

Globale und benutzerspezifische Regelsätze, die Sie dem Modul zugewiesen haben, werden automatisch in den lokalen Regelsatz aufgenommen. Erscheint der Regelsatz am Ende der Regelliste, dann wird er mit der geringsten Priorität bearbeitet. Sie können die Priorität ändern, indem Sie die Position in der Regelliste verändern.

Die Online-Hilfe erläutert Ihnen die Bedeutung der einzelnen Schaltflächen.



4.3.6 IP-Paketfilter-Regeln

Die Bearbeitung von IP-Paketfilter-Regeln erfolgt anhand folgender Auswertungen:

- In der Regel eingetragene Parameter;
- Reihenfolge und der damit verbundenen Priorität der Regel innerhalb des Regelsatzes.

Parameter

Die Projektierung einer IP-Regel beinhaltet folgende Parameter:

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Aktion	Zulassungsfestlegung (Freigabe/Sperre)	• Allow Telegramme gemäß Definition zulassen. • Drop Telegramme gemäß Definition sperren. Für automatisch angelegte Verbindungsregeln: • Allow* • Drop* Wählen Sie diese Regeln, findet kein Abgleich mit STEP 7 statt. Geänderte Regeln werden in SCT also nicht überschrieben.
Von / Nach	Die zugelassenen Kommunikationsrichtungen.	Wird in den folgenden Tabellen beschrieben.
Quell-IP-Adresse	Quell-Adresse der IP-Pakete	Siehe unter Abschnitt "IP-Adressen in IP-Paketfilter-Regeln" in diesem Kapitel. Alternativ können Sie symbolische Namen eingeben.
Ziel-IP-Adresse	Ziel-Adresse der IP-Pakete	

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Dienst	Name des verwendeten IP/ICMP-Dienstes oder der Dienstgruppe. Mit Hilfe der Dienst-Definitionen können Sie Paketfilter-Regeln definieren Sie wählen hier einen der von Ihnen im Dialog IP-Dienste definierten Dienste: - IP-Dienste - ICMP-Dienste Wenn Sie noch keine Dienste definiert haben oder einen weiteren Dienst definieren möchten, betätigen Sie die Schaltfläche "IP/MAC-Dienste-Definition...".	Die Klappliste bietet die projektierten Dienste und Dienstgruppen zur Auswahl an. Keine Angabe bedeutet: es wird kein Dienst geprüft, die Regel gilt für alle Dienste. Hinweis: Damit die vordefinierten IP-Dienste in der Klappliste erscheinen, aktivieren Sie diese zunächst im Standard Modus.
Bandbreite (Mbit/s)	Einstellmöglichkeit für eine Bandbreitenbegrenzung. Kann nur eingegeben werden, wenn bei Aktion "Allow" ausgewählt ist. Ein Paket passiert die Firewall, wenn die Pass-Regel zutrifft und die zulässige Bandbreite für diese Regel noch nicht überschritten worden ist.	CP x43-1 und SCALANCE S < V3.0: 0.001 ... 100 CP 1628 und SCALANCE S ≥ V3.0: 0.001 ... 1000 Für globale und benutzerspezifische Regeln: 0.001 ... 100
Logging	Ein- bzw. Ausschalten des Logging für diese Regel.	
Nr.	Automatisch vergebene Nummer der Regel.	
Kommentar	Platz für eigene Erläuterung der Regel.	Ist ein Kommentare mit "AUTO" gekennzeichnet, wurde er für eine automatische Verbindungsregel angelegt.

Tabelle 4- 11 Richtungen CP

Auswahlmöglichkeiten / Wertebereiche		Security-Modul		Bedeutung
Von	Nach	CP x43-1 Adv.	CP 1628	
Intern	Station	x	-	Zugriff vom internen Netz auf die Station.
	Any	x	-	Zugriff vom internen auf das externe Netz, VPN-Tunnelpartner und die Station.
Extern	Station	x	x	Zugriff vom externen Netz auf die Station.
	Any	x	-	Zugriff vom externen auf das interne Netz und die Station.
Station	Intern	x	-	Zugriff von der Station auf das interne Netz.
	Extern	x	x	Zugriff von der Station auf das externe Netz.
	Tunnel	x	x	Zugriff von der Station auf VPN-Tunnelpartner.

Auswahlmöglichkeiten / Wertebereiche		Security-Modul		Bedeutung
Tunnel	Station	x	x	Zugriff über VPN-Tunnelpartner auf die Station.
	Any	x	-	Zugriff von VPN-Tunnelpartnern auf das interne Netz und die Station.
Any	Extern	x	-	Zugriff vom internen Netz und der Station auf das externe Netz.

Tabelle 4- 12 Richtungen SCALANCE S ≥ V3.0

Auswahlmöglichkeiten / Wertebereiche		Security-Modul		
Von	Nach	S602 V3*	S612 V3**	S623 V3
Intern	Extern	x	x	x
	Tunnel	-	x	x
	Any	-	x	x
	DMZ	-	-	x
Extern	Intern	x	x	x
	Any	-	-	x
	Tunnel	-	-	x
	DMZ	-	-	x
Tunnel	Intern	-	x	x
	Extern	-	x	x
	DMZ	-	-	x
Any	Intern	-	x	x
	Extern	-	-	x
	DMZ	-	-	x
DMZ	Intern	-	-	x
	Extern	-	-	x
	Any	-	-	x
	Tunnel	-	-	x

* Auch für SCALANCE S 602 V2 gültig.

** Auch für SCALANCE S 612 V2 und SCALANCE S 613 V2 gültig.

Reihenfolge bei der Regelauswertung durch das Security-Modul

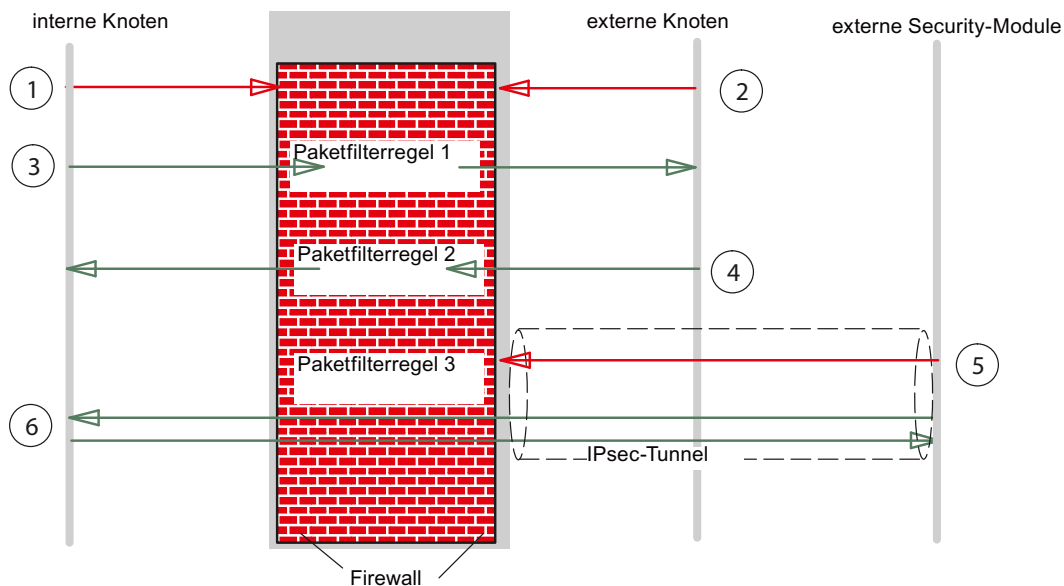
Die Paketfilter-Regeln werden wie folgt ausgewertet:

- Die Liste wird von oben nach unten ausgewertet; bei sich widersprechenden Regeln gilt also immer der weiter oben stehende Eintrag.
- Bei Regeln für die Kommunikation zwischen internem, externen und DMZ-Netz gilt die Abschlussregel: alle Telegramme außer den in der Liste explizit zugelassenen Telegrammen sind gesperrt.
- Bei Regeln für die Kommunikation zwischen internem Netz und IPsec-Tunnel gilt die Abschlussregel: alle Telegramme außer den in der Liste explizit gesperrten Telegrammen sind zugelassen.

Beispiel

[illegible]

Die dargestellten Paketfilter-Regeln bewirken folgendes Verhalten:



- ① Alle Telegrammtypen von intern nach extern sind standardmäßig geblockt, außer den explizit zugelassenen.
- ② Alle Telegrammtypen von extern nach intern sind standardmäßig geblockt, außer den explizit zugelassenen.
- ③ Die IP-Paketfilterregel 1 lässt Telegramme mit der Dienstdefinition "Service X1" von intern nach extern zu.
- ④ Die IP-Paketfilter-Regel 2 lässt Telegramme von extern nach intern zu, wenn erfüllt ist:
 - IP-Adresse des Absenders: 196.65.254.2
 - IP-Adresse des Empfängers: 197.54.199.4
 - Dienstdefinition: "Service X2"
- ⑤ Die IP-Paketfilter-Regel 3 blockt Telegramme mit der Dienstdefinition "Service X1" im VPN (IPsec-Tunnel).
- ⑥ IPsec-Tunnelkommunikation ist standardmäßig zugelassen, außer den explizit geblockten Telegrammtypen.

Siehe auch

MAC-Paketfilter-Regeln (Seite 125)

Wertebereiche IP-Adresse, Subnetzmaske und Adresse des Netzübergangs (Seite 215)

IP-Adressen in IP-Paketfilter-Regeln

Die IP-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; Beispiel: 141.80.0.16

In der Paketfilter-Regel haben Sie folgende Möglichkeiten, IP-Adressen anzugeben:

- keine Angabe
Es erfolgt keine Prüfung, die Regel gilt für alle IP-Adressen.
- eine IP-Adresse
Die Regel gilt genau für die angegebene Adresse.

- Adressband

Die Regel gilt für alle im Adressband erfassten IP-Adressen.

Ein Adressband wird definiert, indem die Anzahl der gültigen Bit-Stellen in der IP-Adresse angegeben wird und zwar in der Form: [IP-Adresse]/[Anzahl der zu berücksichtigenden Bits]

- [IP-Adresse]/24 bedeutet demnach, dass nur die höchstwertigen 24 Bit der IP-Adresse in der Filterregel berücksichtigt werden; das sind die ersten drei Stellen der IP-Adresse.
- [IP-Adresse]/25 bedeutet, dass nur die ersten drei Stellen und das höchstwertige Bit der vierten Stelle der IP-Adresse in der Filterregel berücksichtigt werden.

- Adressbereich

Für die Quell-IP-Adresse kann ein Adressbereich, getrennt durch einen Bindestrich angegeben werden:

[Start-IP-Adresse]-[End-IP-Adresse]

Nähere Informationen finden Sie im Kapitel Wertebereiche IP-Adresse, Subnetzmaske und Adresse des Netzübergangs (Seite 215).

Tabelle 4- 13 Beispiele für Adressband bei IP-Adressen

Quell-IP-Adresse bzw. Ziel-IP-Adresse	Adressband		Anzahl Adressen *)
	von	bis	
192.168.0.0/16	192.168.0.0	192.168.255.255	65.536
192.168.10.0/24	192.168.10.0	192.168.10.255	256
192.168.10.0/25	192.168.10.0	192.168.10.127	128
192.168.10.0/26	192.168.10.0	192.168.10.63	64
192.168.10.0/27	192.168.10.0	192.168.10.31	32
192.168.10.0/28	192.168.10.0	192.168.10.15	16
192.168.10.0/29	192.168.10.0	192.168.10.7	8
192.168.10.0/30	192.168.10.0	192.168.10.3	4
*) Hinweis: Beachten Sie, dass die Adresswerte 0 und 255 in der IP-Adresse Sonderfunktionen haben (0 steht für eine Netzwerkadresse, 255 steht für eine Broadcast-Adresse). Die Anzahl der tatsächlich verfügbaren Adressen verringert sich dadurch.			

4.3.7 IP-Dienste definieren

So erreichen Sie diese Funktion

- Über den Menübefehl "Optionen" > "IP-Dienste".
oder
- Aus dem Register "IP-Regeln" über die Schaltfläche "IP-Dienste".

Bedeutung

Mit Hilfe der IP-Dienst-Definitionen können Sie Firewall-Regeln, die auf bestimmte Dienste angewendet werden, kompakt und übersichtlich definieren. Sie vergeben hierbei einen Namen und ordnen diesem die Dienstparameter zu.

Zusätzlich können Sie so definierte Dienste wiederum unter einem Gruppennamen zu Gruppen zusammenfassen.

Bei der Projektierung der globalen oder lokalen Paketfilter-Regeln verwenden Sie dann einfach diese Namen.

Parameter für IP-Dienste

Die Definition der IP-Dienste erfolgt über folgende Parameter:

Tabelle 4- 14 IP-Dienste: Parameter

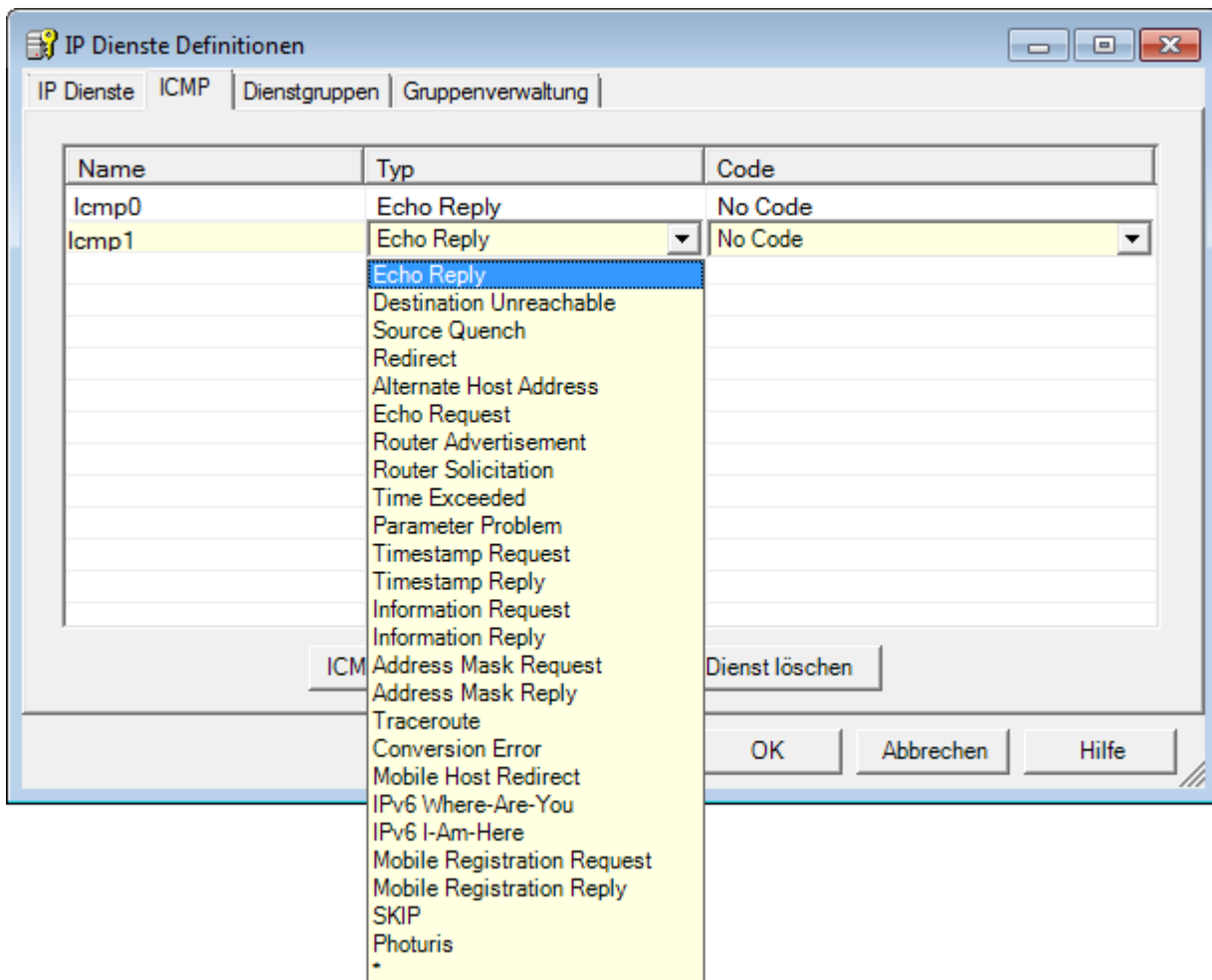
Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Name	Frei definierbarer Name für den Dienst, der zur Identifikation in der Regeldefinition oder in der Gruppenzusammenfassung verwendet wird.	freie Eingabe
Protokoll	Name des Protokolltyps	TCP UDP Any
Quell-Port	Es erfolgt Filterung anhand der hier angegebenen Portnummer; diese definiert den Dienstzugang beim Telegrammabsender.	Beispiele: *: Port wird nicht geprüft 20 bzw. 21: FTP-Service
Ziel-Port	Es erfolgt Filterung anhand der hier angegebenen Portnummer; diese definiert den Dienstzugang beim Telegramm-Empfänger.	Beispiele: *: Port wird nicht geprüft 80: Web-HTTP-Service 102: S7-Protokoll - TCP/Port

4.3.8 ICMP-Dienste definieren

Mit Hilfe der ICMP-Dienst-Definitionen können Sie Firewall-Regeln definieren, die auf bestimmte ICMP-Dienste angewendet werden. Sie vergeben hierbei einen Namen und ordnen diesem die Dienstparameter zu. Die definierten Dienste können Sie unter einem Gruppennamen zu Gruppen zusammenfassen. Bei der Projektierung der Paketfilter-Regeln verwenden Sie dann diese Gruppennamen.

So erreichen Sie diese Funktion

- Über den Menübefehl "Optionen" > "IP-Dienste..." bzw. "MAC-Dienste...", Register "ICMP".
oder
- Über die Schaltfläche "IP-Dienste" bzw. "MAC-Dienste...", Register "ICMP"



Parameter für ICMP-Dienste

Die Definition der ICMP-Dienste erfolgt über folgende Parameter:

Tabelle 4- 15 ICMP-Dienste: Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Name	Frei definierbarer Name für den Dienst, der zur Identifikation in der Regeldefinition oder in der Gruppenzusammenfassung verwendet wird.	Freie Eingabe
Typ	Typ der ICMP-Message	Siehe Dialog-Darstellung.
Code	Codes des ICMP-Types	Werte sind abhängig vom gewählten Typ.

4.3.9 MAC-Paketfilter-Regeln einstellen

Mittels MAC-Paketfilter-Regeln können Sie auf MAC-Telegramme filtern.

Hinweis

Keine MAC-Regeln bei aktiviertem Routing-Modus



Wenn Sie für das SCALANCE S-Modul den Routing-Modus aktiviert haben, finden MAC-Regeln keine Anwendung.

Dialog / Register

Markieren Sie das zu bearbeitende Modul.

Wählen Sie zum Einrichten der Firewall den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Firewall > "MAC-Regeln".

MAC-Paketfilter-Regeln

Die Projektierung einer MAC-Regel beinhaltet folgende Parameter:

Tabelle 4- 16 MAC-Regeln: Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Aktion	Zulassungsfestlegung (Freigabe/Sperre)	- Allow Telegramme gemäß Definition zulassen. - Drop Telegramme gemäß Definition sperren. Für automatisch angelegte Verbindungsregeln: - Allow* - Drop* Wählen Sie diese Regeln, findet kein Abgleich mit STEP 7 statt. Geänderte Regeln werden in SCT also nicht überschrieben.
Von / Nach	Die zugelassenen Kommunikationsrichtungen.	Werden in den folgenden Tabellen beschrieben.
Quell-MAC-Adresse	Quell-Adresse der MAC-Pakete	Alternativ können Sie symbolische Namen eingeben.
Ziel-MAC-Adresse	Ziel-Adresse der MAC-Pakete	
Dienst	Name des verwendeten MAC-Dienstes oder der Dienstgruppe. "Any" fasst die für den einzelnen Eintrag zugelassenen Richtungen zusammen.	Die Klappliste bietet die projektierten Dienste und Dienstgruppen zur Auswahl an. Keine Angabe bedeutet: es wird kein Dienst geprüft, die Regel gilt für alle Dienste. Hinweis: Damit die vordefinierten MAC-Dienste in der Klappliste erscheinen, aktivieren Sie diese zunächst im Standard Modus.
Bandbreite (Mbit/s)	Einstellmöglichkeit für eine Bandbreiten-Begrenzung. Kann nur eingegeben werden, wenn bei Aktion "Allow" ausgewählt ist. Ein Paket passiert die Firewall, wenn die Pass-Regel zutrifft und die zulässige Bandbreite für diese Regel noch nicht überschritten worden ist.	CP x43-1 und SCALANCE S ≤ V3.0: 0.001 ... 100 CP 1628 und SCALANCE S ≥ V3.0: 0.001 ... 1000 Für globale und benutzerspezifische Regeln: 0.001 ... 100
Logging	Ein- bzw. Ausschalten des Logging für diese Regel	
Nr.	Automatisch vergebene Nummer der Regel.	
Kommentar	Platz für eigene Erläuterung der Regel	Ist ein Kommentare mit "AUTO" gekennzeichnet, wurde er für eine automatische Verbindungsregel angelegt.

Erlaubte Richtungen

Folgende Richtungen können eingestellt werden:

Tabelle 4- 17 Firewall-Richtungen CP

Auswahlmöglichkeiten / Wertebereiche		Security-Modul		Bedeutung
Von	Nach	CP x43-1 Adv.	CP 1628	
Extern	Station	x	x	Zugriff vom externen Netz auf die Station.
Station	Extern	x	x	Zugriff von der Station auf das externe Netz.
	Tunnel	x	x	Zugriff von der Station auf VPN-Tunnelpartner.
Tunnel	Station	x	x	Zugriff über VPN-Tunnelpartner auf die Station.

Tabelle 4- 18 Firewall-Richtungen SCALANCE S ≥ V3.0

Auswahlmöglichkeiten / Wertebereiche		Security-Modul		
Von	Nach	S602 V3*	S612 V3**	S623 V3
Intern	Extern	x	x	x
	Tunnel	-	x	x
	Any	-	x	x
	DMZ	-	-	x
Extern	Intern	x	x	x
	Any	-	-	x
	Tunnel	-	-	x
	DMZ	-	-	x
Tunnel	Intern	-	x	x
	Extern	-	x	x
	DMZ	-	-	x
Any	Intern	-	x	x
	Extern	-	-	x
	DMZ	-	-	x
DMZ	Intern	-	-	x
	Extern	-	-	x
	Any	-	-	x
	Tunnel	-	-	x

* Auch für SCALANCE S 602 V2 gültig.

** Auch für SCALANCE S 612 V2 und SCALANCE S 613 V2 gültig.

Regelauswertung durch das Security-Modul

Die Paketfilter-Regeln werden wie folgt ausgewertet:

- Die Liste wird von oben nach unten ausgewertet; bei sich widersprechenden Regeln gilt der weiter oben stehende Eintrag.
- Bei den Regeln für die Kommunikation in Richtung "Intern -> Extern" und "Extern -> Intern" gilt für alle nicht explizit erfassten Telegramme: alle Telegramme sind gesperrt, außer den in der Liste explizit zugelassenen Telegrammen.
- Bei den Regeln für die Kommunikation in Richtung "Intern -> Tunnel" und "Tunnel -> Intern" gilt für alle nicht explizit erfassten Telegramme: alle Telegramme sind zugelassen, außer den in der Liste explizit gesperrten Telegrammen.

ACHTUNG

IP-Regeln greifen für IP-Pakete, MAC-Regeln greifen für Layer-2-Pakete

Für die Firewall können Sie sowohl IP-Regeln als auch MAC-Regeln definieren. Die Bearbeitung in der Firewall ist anhand des Ethertypes des Paketes geregelt.

IP-Pakete werden abhängig von den IP-Regeln weitergeleitet bzw. geblockt und Layer-2-Pakete werden abhängig von den MAC-Regeln weitergeleitet bzw. geblockt.

Es ist nicht möglich, ein IP-Paket mit Hilfe einer MAC-Firewall-Regel beispielsweise hinsichtlich einer MAC-Adresse zu filtern.

Beispiele

Das Beispiel für den IP-Paketfilter in Kapitel 5.4.3 (Seite 116) können Sie sinngemäß auf die MAC-Paketfilter-Regeln anwenden.

4.3.11 MAC-Dienste definieren

So erreichen Sie diese Funktion

- Über den Menübefehl "Optionen" > "MAC-Dienste".
oder
- Aus dem Register "MAC-Regeln" über die Schaltfläche "MAC-Dienste..."

Bedeutung

Mit Hilfe der MAC-Dienst-Definitionen können Sie Firewall-Regeln, die auf bestimmte Dienste angewendet werden, definieren. Sie vergeben einen Namen und ordnen diesem die Dienstparameter zu. Zusätzlich können Sie so definierte Dienste unter einem Gruppennamen zu Gruppen zusammenfassen. Bei der Projektierung der globalen oder lokalen Paketfilter-Regeln verwenden Sie dann diese Namen.

Parameter für MAC-Dienste

Eine MAC-Dienst Definition beinhaltet eine Kategorie protokoll-spezifischer MAC-Parameter:

Tabelle 4- 19 MAC-Dienste Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Name	Frei definierbarer Name für den Dienst, der zur Identifikation in der Regeldefinition oder in der Gruppenzusammenfassung verwendet wird.	freie Eingabe
Protokoll	Name des Protokolltyps: - ISO ISO bezeichnet Telegramme mit folgenden Eigenschaften: Lengthfield <= 05DC (hex), DSAP= userdefined SSAP= userdefined CTRL= userdefined - SNAP SNAP bezeichnet Telegramme mit folgenden Eigenschaften: Lengthfield <= 05DC (hex), DSAP=AA (hex), SSAP=AA (hex), CTRL=03 (hex), OUI=userdefined, OUI-Type=userdefined - PROFINET IO	- ISO - SNAP - PROFINET IO 0x (Code-Eingabe)
DSAP	Destination Service Access Point: LLC-Empfänger-Adresse	
SSAP	Source Service Access Point: LLC-Sender-Adresse	
CTRL	LLC Control Field	
OUI	Organizationally Unique Identifier (die ersten 3 Bytes der MAC Adresse = Hersteller Identifizierung)	
OUI-Typ	Protokoll-Typ/Identifizierung	
*) Die Protokolleingaben 0800 (hex) und 0806 (hex) werden nicht akzeptiert, da diese Werte für IP- bzw. ARP-Telegramme gelten.		

Hinweis

Verarbeitung für S7-CPs

S7-CP

Es werden nur Einstellungen zu ISO-Frames mit DSAP=SSAP=FE (hex) verarbeitet. Andere Frame-Typen sind für S7-CPs nicht relevant und werden daher schon vor der Bearbeitung durch die Firewall verworfen.

Spezielle Einstellungen für SIMATIC NET Dienste

Verwenden Sie für die Filterung spezieller SIMATIC NET Dienste bitte die folgenden SNAP-Einstellungen:

- DCP (Primary Setup Tool):
PROFINET
- SiClock:
OUI= 08 00 06 (hex), OUI-Type= 01 00 (hex)

4.3.12 Dienstgruppen einrichten

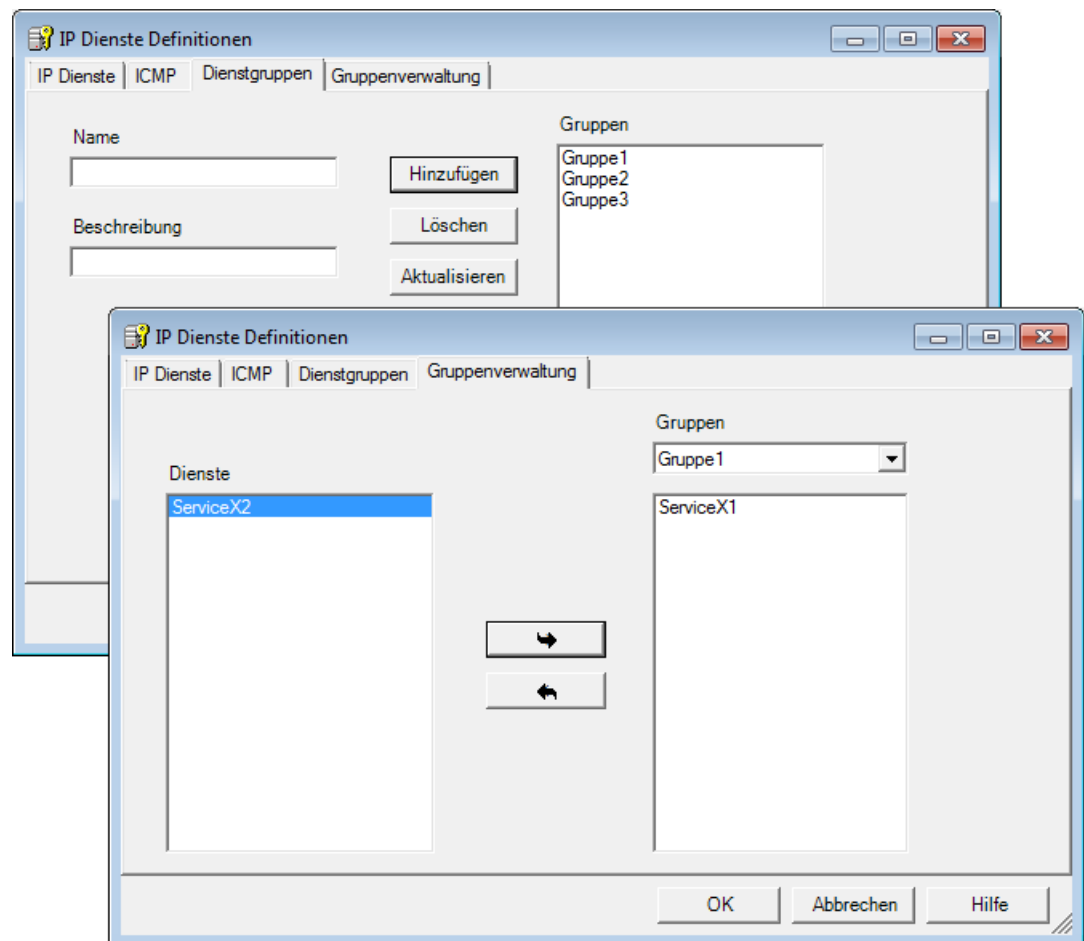
Bildung von Dienstgruppen

Sie können mehrere Dienste durch die Bildung von Dienstgruppen zusammenzufassen. Auf diese Weise können Sie komplexere Dienste aufbauen, die in den Paketfilter-Regeln dann durch einfache Namensauswahl verwendet werden können.

Dialoge / Register

Sie öffnen den Dialog wie folgt:

- Über folgenden Menübefehl "Optionen" > "IP/MAC-Dienst Definition...".
oder
- Aus dem Register "Firewall/IP-Regeln" bzw. "Firewall/MAC-Regeln" über die Schaltfläche "IP/MAC-Dienste-Definition..."



Weitere Moduleigenschaften projektieren

5.1 Security-Modul als Router

5.1.1 Übersicht

Bedeutung

Indem Sie das Security-Modul als Router betreiben, verbinden Sie das interne Netz mit dem externen Netz. Das über das Security-Modul verbundene interne Netz wird somit zu einem eigenen Subnetz.

Sie haben folgende Möglichkeiten:

- Routing - einstellbar im Standard Modus und im Erweiterten Modus
- NAT/NAPT-Routing - einstellbar im Erweiterten Modus

Alle nicht zu einem Subnetz gehörenden Netzwerkanfragen werden durch einen Standard-Router in ein anderes Subnetz weitergeleitet. Siehe Kapitel Standard-Router (Seite 134).

Routing-Modus aktivieren - Register "Schnittstellen"



Wenn Sie den Routing-Modus aktiviert haben, werden die Telegramme weitergeleitet, die an eine im jeweiligen Subnetz (intern oder extern) vorhandene IP-Adresse gerichtet sind. Darüber hinaus gelten die für die jeweilige Übertragungsrichtung getroffenen Firewall-Regeln.

Für diese Betriebsart müssen Sie im Register eine interne IP-Adresse und eine interne Subnetzmaske für die Adressierung des Routers am internen Subnetz projektieren. Alle nicht zu einem Subnetz gehörenden Netzwerkanfragen werden durch den Standard-Router in ein anderes Subnetz weitergeleitet.

Hinweis: Im Gegensatz zum Bridge-Betrieb des Security-Moduls gehen im Routing-Modus VLAN-Tags verloren.

1. Wählen Sie im Register "Schnittstelle" den Routing-Modus als Schnittstellenrouting.
2. Tragen Sie eine interne IP-Adresse und eine interne Subnetzmaske für die Adressierung des Routers am internen Subnetz in die nun aktiven Eingabefelder ein.

5.1.2 Standard-Router



So erreichen Sie diese Funktion

1. Markieren Sie das zu bearbeitende Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Routing".
3. Wenn Sie die Adresse für den Standard-Router eintragen, werden alle Routen über diesen Router geleitet. Wenn Sie keine Adresse für den Standard-Router eintragen, können Sie mehrere spezifische Routen eintragen.
4. Klicken Sie auf die Schaltfläche "Route hinzufügen".
5. Tragen Sie die folgende Werte ein:

Parameter	Funktion	Beispiel-Wert
Netz-ID	Netz-ID des Subnetzes: Anhand der Netz-ID erkennt der Router, ob eine Ziel-Adresse im oder außerhalb des Subnetzes liegt. Darf nicht im gleichen Subnetz liegen wie die IP-Adresse des Security-Moduls.	196.80.96.0
Subnetzmaske	Die Subnetzmaske strukturiert das Netz und dient zur Bildung der Subnetz-ID.	255.255.255.0
Router-IP-Adresse	IP-Adresse des Routers Muss im gleichen Subnetz liegen wie die IP-Adresse des Security-Moduls.	196.80.97.1

Anwendungsbeispiele

S≥V3.0

- Ist im Register "Schnittstellen" die IP-Zuweisung über "PPPoE" konfiguriert, muss kein Standard-Router projiziert werden, da die Standard-Route automatisch immer über die PPPoE-Schnittstelle führt.
- Ist im Register "Schnittstellen" die Adresszuweisung über "Statische Adresse" konfiguriert und ist das Security-Modul über einen DSL-(NAPT-) Router am Internet angeschlossen, muss der DSL-Router als Standard-Router eingetragen werden.

Siehe auch

NAT/NAPT-Routing (Seite 135)

5.1.3 NAT/NAPT-Routing



Voraussetzung

- Das Register "NAT" wird nur angezeigt, wenn Sie sich im Erweiterten Modus befinden.

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.

Abhilfe SCT Standalone: Sie schließen das Projekt, ohne zu speichern und öffnen es erneut.

So erreichen Sie diese Funktion

1. Markieren Sie das zu bearbeitende Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "NAT".
3. Aktivieren Sie je nach Anforderung eine Adressumsetzung gemäß NAT (Network Address Translation) oder NAPT (Network Address Port Translation).
4. Projektieren Sie die Adressumsetzung gemäß den Angaben in den folgenden Kapiteln.

Adressumsetzung mit NAT (Network Address Translation)

NAT ist ein Protokoll zur Adressumsetzung zwischen zwei Adressräumen. Hauptaufgabe ist die Umsetzung von privaten Adressen in Öffentliche, d. h. in IP-Adressen, die im Internet verwendet und auch geroutet werden. Dadurch wird erreicht, dass die Adressen des internen Netzes nach außen im externen Netz nicht bekannt werden. Die internen Teilnehmer sind im externen Netz nur über die in der Adressumsetzungsliste (NAT-Tabelle) festgelegten externen IP-Adresse sichtbar.

Handelt es sich bei der externen IP-Adresse nicht die um Adresse des Security-Moduls und ist die interne IP-Adresse eindeutig, wird dies als 1:1 NAT bezeichnet. Beim 1:1 NAT wird die interne Adresse ohne Portumsetzung auf diese externe Adresse umgesetzt. Ansonsten handelt es sich um n:1 NAT.

Adressumsetzung mit NAPT (Network Address Port Translation)

Die Adressumsetzung bei NAPT verändert die Zieladresse und den Zielport in einer Kommunikationsbeziehung.

5.1 Security-Modul als Router

Umgesetzt werden Telegramme, die vom externen Netz kommen und an die IP-Adresse des Security-Moduls gerichtet sind. Ist der Zielport des Telegramms identisch einem der Werte, der in der Spalte "externer Port" angegeben ist, so ersetzt das Security-Modul die Zieladresse und den Zielport, wie in der entsprechenden Zeile der NAPT-Tabelle angegeben. Bei der Rückantwort setzt das Security-Modul als Quell-IP-Adresse und als Quellport die Werte ein, die beim Initialtelegramm als Zieladresse bzw. Zielport stehen.

Der Unterschied zu NAT liegt darin, dass bei diesem Protokoll auch Ports umgesetzt werden können. Es gibt keine 1:1 Umsetzung der IP-Adresse. Vielmehr existiert nur noch eine öffentliche IP-Adresse, die durch den Zusatz von Portnummern an eine Reihe von privaten IP-Adressen umgesetzt wird.

Konsistenzprüfung - diese Regeln müssen Sie beachten

Beachten Sie für die Adresszuweisung folgende Regeln, um konsistente Einträge zu erhalten:

Prüfung / Regel	Prüfung erfolgt	
	lokal	projektweit
Im Register "Schnittstellen" muss die Netz-ID des internen Subnetzes unterschiedlich zur Netz-ID des externen Subnetzes sein.		x
Die internen IP-Adressen dürfen nicht identisch sein mit den IP-Adressen des Moduls.		x
Übernehmen Sie den durch die Subnetzmaske bestimmten Anteil für die IP-Adressen: - Die externe IP-Adresse muss im selben Subnetzbereich liegen wie die externe IP-Adresse des Security-Moduls im Register "Schnittstellen". - Die interne IP-Adresse muss im selben Subnetzbereich liegen wie die interne IP-Adresse des Security-Moduls im Register "Schnittstellen".		x
Eine IP-Adresse, die in der NAT/NAPT-Adressumsetzungsliste verwendet wird, darf keine Multicast-Adresse und keine Broadcast-Adresse sein.		x
Der Standard-Router muss in einem der beiden Subnetze des Security-Moduls liegen d. h., er muss entweder zur externen oder zur internen IP-Adresse passen.		x
Die für die NAPT-Umsetzung vergebenen externen Ports liegen im Bereich > 0 und ≤ 65535 . Port 123 (NTP), 443 (HTTPS), 514 (Syslog) und 500+4500 (IPsec) sind davon ausgeschlossen.	x	
Die externe IP-Adresse des Security-Moduls darf in der NAT-Tabelle nur für die Richtung "Scr-NAT (nach Extern)" verwendet werden.	x	
Die interne IP-Adresse des Security-Moduls darf in der NAT-Tabelle und in der NAPT-Tabelle nicht verwendet werden.		x
Duplikatsprüfung in der NAT-Tabelle Eine externe IP-Adresse, die mit Richtung "Dst-NAT (von Extern)" oder "Src-NAT +Dst-NAT (Extern)" verwendet wird, darf nur einmal in der NAT-Tabelle erscheinen.	x	

Prüfung / Regel	Prüfung erfolgt	
	lokal	projektweit
Duplikatsprüfung in der NAPT-Tabelle - Eine externe Portnummer darf nur einmal eingetragen sein. Da immer die IP-Adresse des Security-Moduls als externe IP-Adresse verwendet wird, wäre bei mehrfacher Verwendung keine Eindeutigkeit gegeben. - Die Portnummern bzw. Portbereiche der externen Ports dürfen sich nicht überschneiden.	x	
Sobald der Routing-Modus aktiviert wurde, müssen dem Security-Modul die internen Adressen (IP/Subnetz) zugeordnet werden.	x	
Interne NAPT-Ports können im Bereich > 0 und ≤ 65535 liegen.	x	



Siehe auch

Führen Sie nach Abschluss Ihrer Eingaben eine Konsistenzprüfung durch.
Wählen Sie hierzu den Menübefehl "Optionen" > "Konsistenzprüfungen".

Standard-Router (Seite 134)

5.1.4 Adressumsetzung mit NAT/NAPT

NAT aktivieren

Der Eingabebereich für NAT wird aktiviert. NAT-Adressumsetzungen werden erst durch die nachfolgend beschriebene Option und Einträge in die Adressumsetzungsliste wirksam. Zusätzlich müssen Sie die Firewall passend konfigurieren.

Die IP-Adressumsetzung kann über die folgenden Schnittstellen erfolgen:

- Extern: Die Adressumsetzung erfolgt am externen Port

Die IP-Adressumsetzung kann in folgende Richtungen erfolgen:

- Destination NAT (Dst-NAT): Die IP-Adressumsetzung erfolgt von extern nach intern. Vom externen Subnetz kommende Telegramme werden auf die angegebene externe IP-Adresse geprüft und mit der angegebenen internen IP-Adresse in das interne Netz weitergeleitet. Der Zugriff von extern nach intern über die externe Adresse ist möglich.
- Source NAT (Src-NAT): Die IP-Adressumsetzung erfolgt von intern nach extern. Vom internen Subnetz kommende Telegramme werden auf die angegebene interne IP-Adresse geprüft und mit der angegebenen externen IP-Adresse in das externe Netz weitergeleitet. Der Zugriff von intern nach extern ist möglich. Am externen Netz wirkt die externe Adresse.
- Source- und Destination NAT (Src-NAT + Dst-NAT): Die IP-Adressumsetzung kann von intern oder extern erfolgen. Der Zugriff von intern und extern ist möglich. Am externen Netz wirkt die externe Adresse.

Eingabemöglichkeiten für Adressumsetzung am externen Port

Soll die Adressumsetzung am externen Port erfolgen, stehen Ihnen die folgenden Eingabemöglichkeiten zur Verfügung.

Umsetzungsart "Dst-NAT (von Extern)"

Feld	Mögliche Eingaben	Bedeutung
Externe IP-Adresse	IP-Adresse im externen Subnetz Bei dynamischer Adressevergabe funktioniert diese Umsetzungsart nicht.	Ziel-IP-Adresse im externen Netz, über die auf eine IP-Adresse im internen Subnetz zugegriffen werden soll. Stimmt in einem Telegramm die Zieladresse mit der eingegebenen Adresse überein, wird die Adresse durch die entsprechende interne IP-Adresse ausgetauscht. Handelt es bei der hier eingegebenen Adresse nicht um die IP-Adresse des Security-Moduls, wird diese zur Alias-Adresse. Dies bedeutet, dass die angegebene Adresse zusätzlich als Adresse am ausgewählten Port registriert wird. Stellen Sie sicher, dass mit dieser Adresse keine IP-Adresskonflikt besteht.
Interne IP-Adresse	IP-Adresse im internen Subnetz	Die Ziel-IP-Adresse wird durch interne IP-Adresse ersetzt. Die Adressumsetzung erfolgt von extern nach intern.

Umsetzungsart "Src-NAT (nach Extern)"

Feld	Mögliche Eingaben	Bedeutung
Externe IP-Adresse	- IP-Adresse im externen Subnetz - IP-Adresse vom Security-Modul, falls die Option "Freigabe für alle internen Teilnehmer zulassen" nicht aktiviert ist. Bei dynamischer Adressevergabe ist keine Eingabe möglich.	Eingabe der IP-Adresse, die als neue Quell-IP-Adresse verwendet werden soll. Handelt es bei der hier eingegebenen Adresse nicht um die IP-Adresse des Security-Moduls, wird diese zur Alias-Adresse. Dies bedeutet, dass die angegebene Adresse zusätzlich als Adresse am ausgewählten Port registriert wird. Stellen Sie sicher, dass mit dieser Adresse keine IP-Adresskonflikt besteht.
Interne IP-Adresse	IP-Adresse im internen Subnetz	Die Quell-IP-Adresse des angegebenen internen Teilnehmers wird durch die angegebene externe Adresse ersetzt. Die IP-Adressumsetzung erfolgt also von intern nach extern.
	Subnetz bzw. IP-Adressbereich	Die Quell-IP-Adressen aus dem angegebenen Subnetz oder IP-Adressbereich werden durch die externe IP-Adresse ersetzt. Der Quellport wird ersetzt. Der Bereich wird durch einen Bindestrich getrennt eingegeben.

Zusätzlich kann die folgende Funktion aktiviert werden:

- Freigabe für alle internen Teilnehmer zulassen

Indem Sie diese Option wählen, erfolgt für alle von intern nach extern gehenden Telegramme eine Umsetzung der internen IP-Adresse auf die externe Modul IP-Adresse und einer zusätzlich vom Modul vergebenen Port-Nummer. Die Verwendung der IP-Adresse der externen Schnittstelle in der Spalte "externe IP-Adresse" ist dann nicht mehr zulässig.

Dieses Verhalten wird an der in der NAT-Tabelle unten zusätzlich eingeblendeten Zeile sichtbar. Dort wird mit einem Symbol "*" in der Spalte "interne IP-Adresse" angezeigt, dass alle von intern nach extern gerichteten Telegramme umgesetzt werden.

Anmerkung: Wegen dieser Auswirkung auf die Adressumsetzungsliste ist diese Option trotz der zusätzlichen Zuordnung einer Portnummer dem Eingabebereich NAT zugeordnet.

Umsetzungsart "Src-NAT + Dst-NAT (Extern)"

Feld	Mögliche Eingaben	Bedeutung
Externe IP-Adresse	IP-Adresse im externen Subnetz Bei dynamischer Adressevergabe funktioniert diese Umsetzungsart nicht.	Erfolgt die Adressumsetzung von intern nach extern: siehe Tabelle "Umsetzungsart Dst-NAT (von Extern)"
Interne IP-Adresse	IP-Adresse im internen Subnetz	Erfolgt die Adressumsetzung von extern nach intern: siehe Tabelle "Umsetzungsart Src-NAT (nach Extern)"

NAPT aktivieren

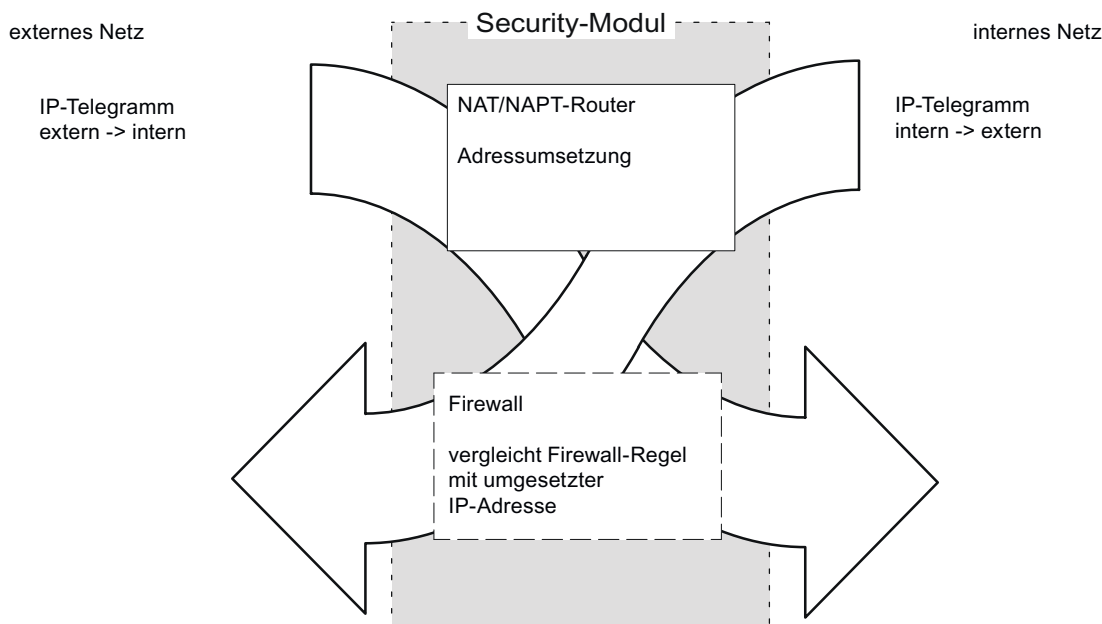
Der Eingabebereich für NAPT wird aktiviert. NAPT-Umsetzungen werden erst durch die nachfolgend beschriebene Option und Einträge in die Liste wirksam. Zusätzlich müssen Sie die Firewall passend konfigurieren (siehe Beispiele).

Feld	Mögliche Eingaben	Bedeutung
externer Port	Port oder Portbereich Beispiel für die Eingabe eines Portbereiches: 78:99	Ein Teilnehmer im externen Netz kann einem Teilnehmer im internen Subnetz ein Telegramm senden, indem er diese Portnummer verwendet.
interne IP-Adresse	Siehe Kapitel "IP-Adressen in IP-Paketfilter-Regeln". Alternativ können Sie symbolische Namen eingeben.	IP-Adresse des angesprochenen Teilnehmers im internen Subnetz.
interner Port	Port	Portnummer eines Teilnehmers im internen Subnetz.

5.1.5 Zusammenhang zwischen NAT/NAPT-Router und Firewall

Zusammenhang zwischen NAT/NAPT-Router und Firewall

Network Address Translation (NAT) verändert die IP-Adressen und eventuell die Portnummern in IP-Telegrammen. Die Adressen werden geändert, bevor die Firewall die IP-Telegramme filtert, d. h. die IP-Adressen und eventuell die Portnummern werden geändert, bevor die Filterung erfolgt.



ACHTUNG

Abstimmen von NAT/NAPT-Einstellungen und Firewall-Regeln

Stimmen Sie die Einstellungen für den NAT/NAPT-Router und die Firewall-Regeln so aufeinander ab, dass Telegramme mit umgesetzter Adresse die Firewall passieren können.

Stateful Packet Inspection

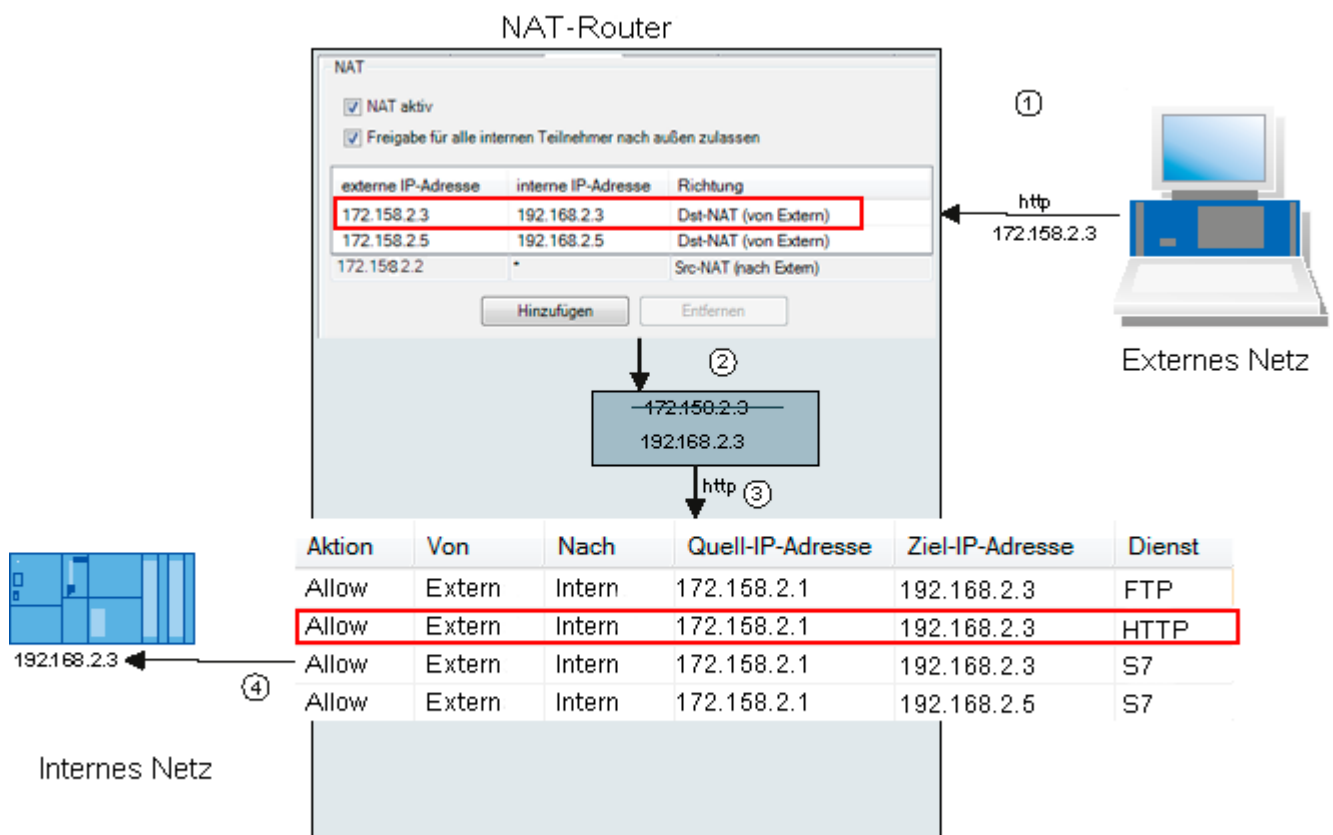
Firewall und NAT/NAPT-Router unterstützen den Mechanismus "Stateful Packet Inspection". Daher können Antworttelegramme den NAT/NAPT-Router und die Firewall passieren, ohne dass deren Adressen in der Firewall-Regel und der NAT/NAPT-Adressumsetzung zusätzlich aufgenommen werden müssen.

5.1.6 1:1 NAT-Routing - Beispiele zur Konfiguration Teil 1

Was soll in dem Beispiel gezeigt werden

Von dem PC mit der Adresse 172.158.2.1 soll auf die Steuerung mit der Adresse 192.168.2.3 im internen Netz zugegriffen werden. Da die Adresse 192.168.2.3 keine öffentliche Adresse ist, muss diese vom NAT-Router auf eine zusätzliche öffentliche Adresse (Alias Adresse, hier 172.158.2.3) umgesetzt werden. Mit der Firewall wird sichergestellt, dass der PC nur auf die Dienste FTP, HTTP und S7 der Steuerung zugreifen kann.

Schematischer Ablauf



NAT Umsetzung	Aktion
①	Ein Gerät aus dem externen Netz will ein Datenpaket an die 172.158.2.3 schicken (HTTP-Anwendung).
②	Der NAT-Router übersetzt die Adresse anhand der NAT-Tabelle in die private IP-Adresse 192.168.2.3
③	Die Firewall prüft, wie es das Datenpaket behandeln soll. Durch den Eintrag "Allow" > "Extern" nach "Intern" > "192.168.2.3" > "HTTP" dürfen alle Datenpakete, die vom PG über Port 80 kommen und an 192.168.2.3 adressiert sind, passieren.

NAT Umsetzung	Aktion
④	Das Datenpaket wird in das interne Netz geleitet.
⑤	Durch die "Stateful-Inspektion"-Funktion der Firewall werden die Antworttelegramme automatisch weitergeleitet.

5.1.7 NAT/NAPT-Routing - Beispiele zur Konfiguration Teil 2

Übersicht

Sie finden in diesem Kapitel folgende Beispiele zur Konfiguration des NAT/NAPT-Routers:

- **Beispiel 1: NAT-Adressumsetzung "Dst-NAT (von Extern)"**

Anwendungsfall: Das interne Netz ist ein privates Subnetz. Es soll auf einen internen Teilnehmer, z. B. eine CPU 300 als i-Device, zugegriffen werden. Von der Leitebene aus soll die Web Diagnose oder das Herunterladen von STEP 7-Daten erlaubt sein. Von der S7300-Station darf nicht auf die Leitebene zugegriffen werden.

- **Beispiel 2: NAT-Adressumsetzung "Scr-NAT (nach Extern)"**

Anwendungsfall: Das interne Netz ist ein privates Subnetz. Teilnehmer im internen Netz ist ein Gerät, z. B. eine CPU 300 als i-Device, das seine Uhrzeit über einen NTP-Server im Internet synchronisieren möchte. Von der Leitebene aus soll die Web Diagnose oder das Herunterladen von STEP 7 Daten erlaubt sein.

- **Beispiel 3: NAT-Adressumsetzung "Src-NAT + Dst-NAT (Extern)"**

Anwendungsfall: Das interne Netz ist ein privates Subnetz. Von der Leitebene aus soll der Zugriff auf ausgewählte Teilnehmer zugelassen werden. Die ausgewählten Teilnehmer sollen ebenfalls auf die Leitebene zugreifen können.

- **Beispiel 4: NAPT-Adressumsetzung**

Projektierung

In der folgenden Routing-Projektierung finden Sie Adresszuweisungen gemäß NAT- und NAPT-Adressumsetzung:

Moduleigenschaften - Modul2

NAT

☒ NAT aktiv

☐ Freigabe für alle internen Teilnehmer nach außen zulassen

externe IP-Adresse	interne IP-Adresse	Richtung
192.168.10.123	192.168.12.3	Dest-NAT (von Extern)
192.168.10.124	192.168.12.3	Src-NAT (nach Extern)
192.168.10.101	192.168.12.4	Src-NAT+Dest-NAT (Extern)

NAPT

☒ NAPT aktiv

Extern (P1): 192.168.10.2, Intern (P2): 192.168.10.23

externer Port	interne IP-Adresse	interner Port	Schnittstelle
8000	192.168.12.5	345	Extern

IP-Regeln

Aktion	Von	Nach	Quell-IP-Adresse	Ziel-IP-Adresse	Dienst	Bandbreite (Mbit/s)	Logging	Nr.	Kommentar
Allow	Extern	Intern		192.168.12.3	(alle)			IP-R_1	
Allow	Intern	Extern	192.168.10.124	192.168.10.11	(alle)			IP-R_2	
Allow	Extern	Intern		192.168.12.4	(alle)			IP-R_3	
Allow	Intern	Extern	192.168.10.101		(alle)			IP-R_4	
Allow	Extern	Intern		192.168.12.5	OpenP345			IP-R_5	

Beschreibung

- **Beispiel 1: NAT-Adressumsetzung "Dst-NAT (von Extern)"**

Ein Teilnehmer im externen Netz kann mit dem Teilnehmer mit der internen IP-Adresse 192.168.12.3 im internen Subnetz kommunizieren, indem er die externe IP-Adresse 192.168.10.123 als Zieladresse verwendet.

- **Beispiel 2: NAT-Adressumsetzung "Scr-NAT (nach Extern)"**

Telegramme eines internen Teilnehmers mit der internen IP-Adresse 192.168.12.3 werden in das externe Netz mit der externen IP-Adresse 192.168.10.124 als Quelladresse weitergeleitet. Die Firewall ist im Beispiel so eingestellt, dass die Kommunikation mit der Quell-IP-Adresse 192.168.10.124 von intern nach extern zugelassen ist und mit dem Teilnehmer mit

der IP-Adresse 192.168.10.11 kommunizieren werden kann.

- **Beispiel 3: NAT-Adressumsetzung "Src-NAT + Dst-NAT (Extern)"**

In diesem Beispiel wird die Adressumsetzung sowohl bei intern als auch extern eingehenden Telegrammen wie folgt vorgenommen:

- Ein Teilnehmer im externen Netz kann dem Teilnehmer mit der internen IP-Adresse 192.168.12.4 im internen Subnetz kommunizieren, indem er die externe IP-Adresse 192.168.10.101 als Zieladresse verwendet.
- Telegramme eines internen Teilnehmers mit der internen IP-Adresse 192.168.12.4 werden am externen Netz mit der externen IP-Adresse 192.168.10.101 als Quelladresse weitergeleitet. Die Firewall ist so eingestellt, dass Telegramme mit der Quell-IP-Adresse 192.168.10.101 von intern nach extern zugelassen sind.

- **Beispiel 4: NAPT-Adressumsetzung**

Adressumsetzungen erfolgen gemäß NAPT so, dass es jeweils zusätzlich Portnummern zugewiesen werden. Alle auf dem externen Netz eingehenden TCP- und UDP-Telegramme werden auf ihre Ziel-IP-Adresse und Ziel-Portnummer überprüft.

- Ein Teilnehmer im externen Netz kann dem Teilnehmer mit der IP-Adresse 192.168.12.5 und Portnummer 345 im internen Subnetz ein Telegramm senden, indem er als Ziel-Adresse die externe Modul-IP-Adresse 192.168.10.1 und die externe Portnummer 8000 verwendet.

5.1.8 NAT/NAPT-Routing - Beispiele zur Konfiguration Teil 3

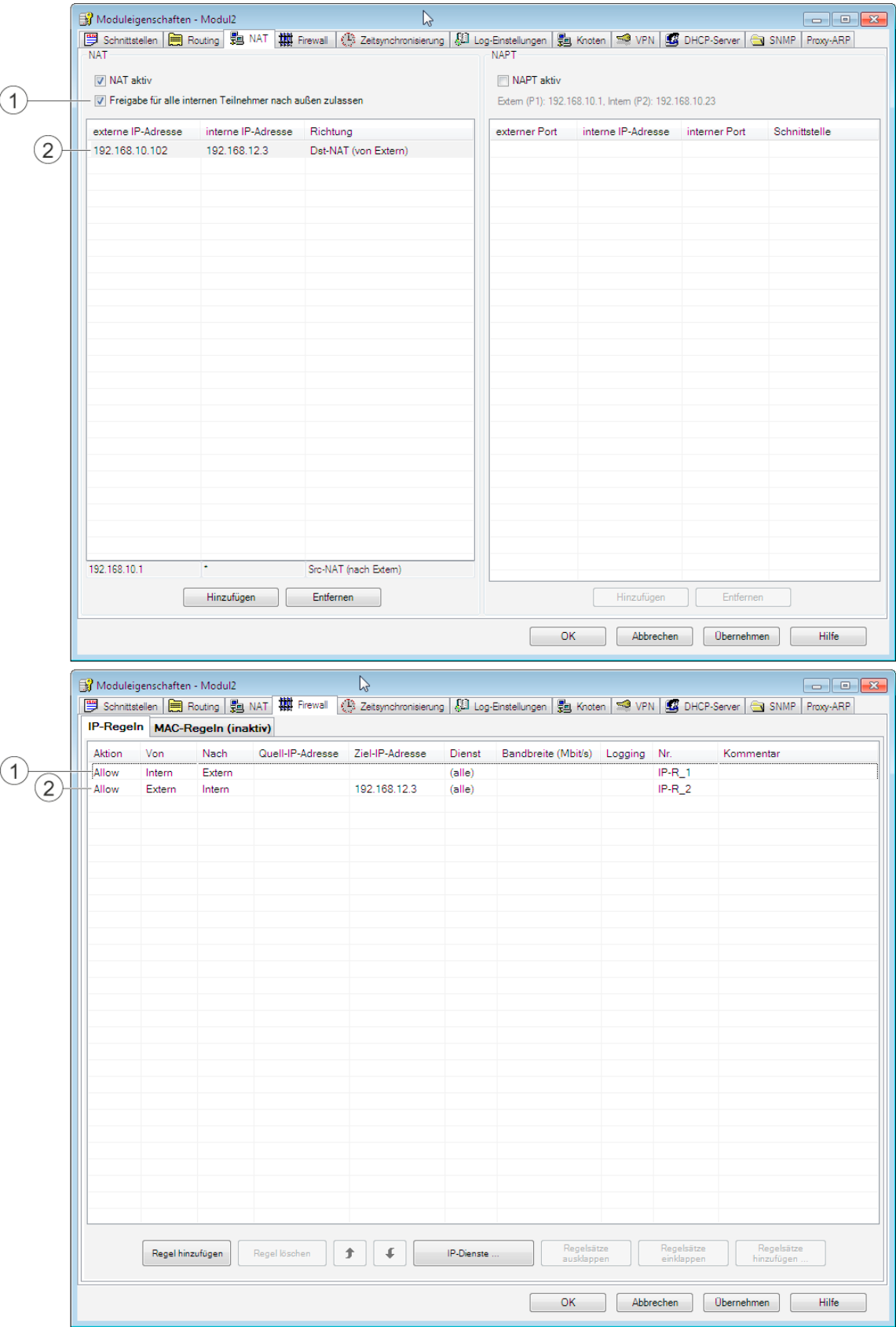
Übersicht

Sie finden in diesem Kapitel folgende Beispiele zur Konfiguration des NAT/NAPT-Routers:

- Beispiel 1: Alle internen Teilnehmer für externe Kommunikation zulassen
- Beispiel 2: Zusätzlich Telegramme zulassen, die von extern nach intern gerichtet sind.

Projektierung

In der folgenden Routing-Projektierung finden Sie Adresszuweisungen gemäß NAT-Adressumsetzung:



Beschreibung

Beispiel 1 - Alle internen Teilnehmer für externe Kommunikation zulassen

Im Dialogbereich "NAT" ist das Optionskästchen "Freigabe für alle internen Teilnehmer nach außen zulassen" aktiviert.

Damit ist die Kommunikation von intern nach extern möglich. Die Adressumsetzung erfolgt hierbei so, dass alle internen Adressen auf die externe IP-Adresse des Security-Moduls und jeweils einer dynamisch vergebenen Portnummer umgesetzt werden.

Eine Richtungsangabe in der NAT-Adressumsetzungsliste ist nun nicht mehr relevant. Sämtliche weiteren Angaben beziehen sich auf die Kommunikationsrichtung extern nach intern.

Zusätzlich ist die Firewall so eingestellt, dass die Telegramme von intern nach extern passieren können.

Beispiel 2 - Zusätzlich Telegramme zulassen, die von extern nach intern gerichtet sind.

Um zusätzlich zum Beispiel 1 die Kommunikation von extern nach intern zuzulassen, sind Angaben in der NAT- oder in der NAPT-Adressumsetzungsliste einzutragen. Der Eintrag im Beispiel besagt, dass Telegramme an den Teilnehmer mit der IP-Adresse 192.168.10.102 auf die interne IP-Adresse 192.168.12.3 umgesetzt werden.

Entsprechend muss die Firewall eingestellt werden. Da immer zunächst die NAT/NAPT-Umsetzung erfolgt und erst im zweiten Schritt die umgesetzte Adresse in der Firewall geprüft wird, ist im Beispiel die interne IP-Adresse als Ziel-IP-Adresse in der Firewall eingetragen.

5.2 Security-Modul als DHCP-Server

5.2.1 Übersicht



Übersicht

Sie können das Security-Modul am internen Netz als DHCP-Server (DHCP = Dynamic Host Configuration Protokoll) betreiben. Damit ist es möglich, den am internen Netz angeschlossenen Geräten automatisch IP-Adressen zuzuweisen.

Die IP-Adressen werden hierbei entweder dynamisch aus einem von Ihnen vergebenen Adressband verteilt oder es wird gemäß Ihrer Vorgabe eine bestimmte IP-Adresse einem bestimmten Gerät zugewiesen.

DHCP-Server für DMZ

S623

Um auch Geräten in der DMZ eine dynamische IP-Adresse zuweisen zu können, kann auf dem DMZ-Port ein DHCP-Server aktiviert werden. Damit die Geräte in der DMZ für die Firewall-Konfiguration immer die gleiche IP-Adresse bekommen, darf die Adresszuordnung nur statisch anhand der MAC-Adresse oder anhand der Client-ID erfolgen.

Voraussetzung

Sie müssen die Geräte am internen Netz so konfigurieren, dass diese die IP-Adresse von einem DHCP-Server beziehen.

Je nach Betriebsart übermittelt das Security-Modul den Teilnehmern im Subnetz eine IP-Adresse des Standard-Router oder Sie müssen den Teilnehmern im Subnetz eine Router IP-Adresse bekannt machen.

- Router IP-Adresse wird übermittelt

In folgenden Fällen wird durch das DHCP-Protokoll vom Security-Modul eine Router IP-Adresse an den Teilnehmer übermittelt:

- Das Security-Modul ist für den Router-Betrieb konfiguriert

Das Security-Modul übermittelt in diesem Fall die eigene IP-Adresse als Router IP-Adresse.

- Das Security-Modul ist nicht für den Router-Betrieb konfiguriert, es ist aber in der Konfiguration vom Security-Modul ein Standard-Router angegeben

Das Security-Modul übermittelt in diesem Fall die IP-Adresse des Standard-Routers als Router-IP.

- Router IP-Adresse wird nicht übermittelt

Tragen Sie in folgenden Fällen die Router IP-Adresse beim Teilnehmer manuell ein:

- Das Security-Modul ist nicht für den Router-Betrieb konfiguriert;
- In der Konfiguration vom Security-Modul ist kein Standard-Router angegeben.

Siehe auch

Konsistenzprüfungen (Seite 52)

5.2.2 DHCP-Server konfigurieren

Voraussetzung

Das Register "DHCP-Server" wird nur angezeigt, wenn Sie den Erweiterten Modus eingeschaltet haben.

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.

Abhilfe SCT Standalone: Sie schließen das Projekt, ohne zu speichern und öffnen es erneut.

So erreichen Sie diese Funktion

1. Markieren Sie das zu bearbeitende Modul.

2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "DHCP-Server".

Moduleigenschaften - S623-V3

Schnittstellen Routing NAT Firewall Zeitsynchronisierung Log-Einstellungen Knoten VPN DHCP-Server SNMP Proxy-ARP

☒ DHCP aktivieren

Einstellungen für Schnittstelle

Intern

Statische Adresszuordnungen

MAC-Adresse	Client-ID	IP-Adresse
02-02-03-03-04-04		200.1.2.195
02-02-03-03-04-05		200.1.2.198

Hinzufügen Entfernen

Dynamische Adresszuordnungen

Geben Sie den gewünschten Adressbereich ein:

Startadresse: 200.1.2.200 Endadresse: 200.1.2.220

☒ Erweiterter Modus

OK Abbrechen Übernehmen Hilfe

3. Aktivieren Sie das Kontrollkästchen "DHCP aktivieren".
4. Wählen Sie aus, für welche Schnittstelle die DHCP-Einstellungen vorgenommen werden sollen.
5. Nehmen Sie die Adresszuordnung vor. Sie haben die beiden folgenden Möglichkeiten zur Konfiguration:

- Statische Adresszuordnung

Geräten mit einer bestimmten MAC-Adresse oder Client-ID werden jeweils vorgegebene IP-Adressen zugeordnet. Tragen Sie hierzu diese Geräte in die Adressliste im Eingabebereich "Statische Adresszuordnung" ein.

- Dynamische Adresszuordnung

Geräte, deren MAC-Adresse oder deren Client-ID nicht explizit angegeben wurde, erhalten eine beliebige IP-Adresse aus einem vorgegebenen Adressband. Dieses Adressband stellen Sie im Eingabebereich "Dynamische Adresszuordnungen" ein.

ACHTUNG

Dynamische Adressvergabe - Verhalten nach Unterbrechung der Spannungsversorgung

Beachten Sie, dass die dynamisch vergebenen IP-Adressen nicht gespeichert werden, wenn die Spannungsversorgung unterbrochen wird. Nach Wiederkehr der Spannungsversorgung müssen Sie daher dafür sorgen, dass die Teilnehmer erneut eine IP-Adresse anfordern.

Sie sollten daher die dynamische Adressvergabe nur für folgende Teilnehmer vorsehen:

- Teilnehmer, die im Subnetz temporär genutzt werden (wie beispielsweise Service-Geräte);
- Teilnehmer, die eine einmal zugewiesene IP-Adresse bei einer erneuten Anforderung an den DHCP-Server als "Vorzugsadresse" übermitteln (wie beispielsweise PC-Stationen).

Für die Teilnehmer im dauernden Betrieb ist die statische Adresszuweisung über die Angabe einer Client-ID (empfohlen für S7 CPs wegen des einfacheren Baugruppentaustechs) oder der MAC-Adresse vorzuziehen.

Symbolische Namen werden unterstützt

Sie können in der hier beschriebenen Funktion die IP- oder MAC-Adressen auch als symbolische Namen eingeben.

Konsistenzprüfung - diese Regeln müssen Sie beachten

Berücksichtigen Sie bei Ihrer Eingabe die nachfolgend aufgeführten Regeln.

Prüfung / Regel	Prüfung erfolgt ¹⁾	
	lokal	Projekt-/Modulweit
Die in der Adressliste im Eingabebereich "Statische Adresszuordnung" zugewiesenen IP-Adressen dürfen nicht im Bereich der dynamischen IP-Adressen liegen.		x
Symbolische Namen müssen eine numerische Adresszuordnung besitzen. Wenn Sie symbolische Namen hier neu vergeben, müssen Sie noch die Adresszuordnung im Dialog "Symbolische Namen" vornehmen.		x

Prüfung / Regel	Prüfung erfolgt ¹⁾	
	lokal	Projekt-/Modulweit
IP-Adressen, MAC-Adressen und Client-IDs dürfen in der Tabelle "statische IP-Adressen" nur einmal vorkommen (bezogen auf das Security-Modul).		x
Sie müssen bei den statisch zugewiesenen IP-Adressen entweder die MAC-Adresse oder die Client-ID (Rechnername) angeben.	x	
Die Client-ID ist eine Zeichenfolge mit maximal 63 Zeichen. Es dürfen nur die folgenden Zeichen verwendet werden: a-z, A-Z, 0-9 und - (Bindestrich). Hinweis Bei SIMATIC S7 kann den Geräten an der Ethernet-Schnittstelle für den Bezug einer IP-Adresse über DHCP eine Client-ID zugewiesen werden. Bei PCs ist die Vorgehensweise abhängig vom verwendeten Betriebssystem; empfohlen wird, hier die MAC-Adresse für die Zuordnung zu verwenden.	x	
Sie müssen bei den statisch zugewiesenen IP-Adressen die IP-Adresse angeben.	x	
Folgende IP-Adressen dürfen nicht im Bereich des freien IP-Adressbereichs (dynamische IP-Adressen) liegen: • alle Router-Adressen im Register "Routing" • NTP-Server • Syslog-Server • Standard-Router • Security-Modul Adresse(n)		x
DHCP wird vom Security-Modul an der Schnittstelle zum internen Subnetz unterstützt. Aus diesem Betriebsverhalten des Security-Moduls ergeben sich weiterhin für IP-Adressen im Bereich des freien IP-Adressbereichs (dynamische IP-Adressen) folgende Anforderungen: • Bridge Modus Der Bereich des freien IP-Adressbereichs muss in dem durch das Security-Modul definierten Netz liegen. • Routing Modus Der Bereich des freien IP-Adressbereichs muss in dem durch das Security-Modul definierten internen Subnetz liegen.		x
Der freie IP-Adressbereich muss durch die Angabe der Start-IP-Adresse und der End-IP-Adresse vollständig angegeben sein. Die End-IP-Adresse muss größer als die Start-IP-Adresse sein.	x	
Die IP-Adressen, die Sie in die Adressliste im Eingabebereich "Statische Adresszuordnung" eingeben, müssen im Adressbereich des internen Subnetzes des Security-Moduls liegen.		x

Legende:

¹⁾ Beachten Sie die Erläuterungen im Kapitel Konsistenzprüfungen (Seite 52).

5.3 Zeitsynchronisierung

5.3.1 Übersicht

Bedeutung

Zur Überprüfung der zeitlichen Gültigkeit eines Zertifikates und für die Zeitstempel von Log-Einträgen wird auf dem Security-Modul Datum und Uhrzeit geführt.

Projektierbar sind folgende Alternativen:

- Automatisches Stellen der Modul-Uhrzeit mit der PC-Uhrzeit beim Laden einer Konfiguration. SCA
- Automatisches Stellen und periodischer Abgleich der Uhrzeit über einen Network Time Protocol-Server (NTP-Server).

Hinweis

Die Zeitsynchronisation bezieht sich lediglich auf das Security-Modul und kann nicht zur Synchronisation von Geräten im internen Netz des Security-Moduls verwendet werden.

Synchronisierung durch einen NTP-Server

ACHTUNG
Telegramme explizit freigeben Wenn der NTP-Server vom Security-Modul nicht erreichbar ist, müssen Sie die Telegramme des NTP-Servers in der Firewall explizit freigeben (UDP, Port 123).

Beim Anlegen des NTP-Servers gelten die folgenden Regeln:

- NTP-Server können über das SCT-Menü "Optionen" > "Definition der NTP-Server" projektweit angelegt werden. Weisen Sie einen NTP-Server über das Eigenschaften-Register "Zeitsynchronisation" einem Security-Modul zu. Verwenden verschiedene Security-Module im SCT-Projekt den selben NTP-Server, so müssen dessen Daten nur einmal eingegeben werden.
- Sie können projektweit 32 NTP-Server anlegen.
- Sie können einem Security-Modul max. 4 NTP-Server zuweisen.
- Symbolische Namen für die IP-Adresse des NTP-Servers werden nicht unterstützt.
- Von bereits in STEP 7 angelegten NTP-Servern wird die IP-Adresse und das Aktualisierungsintervall nach SCT migriert. CP
- Bei Auswahl von "NTP (gesichert)", akzeptiert das Security-Modul nur die Zeit von entsprechend konfigurierten gesicherten NTP-Servern. Eine gemischte Konfiguration von ungesicherten und gesicherten NTP-Servern auf einem Security-Modul ist nicht möglich.

CP

5.3.2 Uhrzeitführung konfigurieren

So erreichen Sie diese Funktion

Menübefehl SCT: "Optionen" > "Definition der NTP-Server...".

Menübefehl STEP 7 (wenn die Option "Uhrzeitsynchronisation im NTP Verfahren einschalten" aktiviert ist): "Uhrzeitsynchronisation" > "Erweiterte NTP-Konfiguration aktivieren", Schaltfläche "Ausführen".

Alternativen der Zeitsynchronisation

Projektierbar sind folgende Alternativen:

Tabelle 5- 1 Zeitsynchronisation für CP

Auswahlmöglichkeit	Bedeutung / Auswirkung
Keine Zeitsynchronisation	Keine Zeitsynchronisation über den PC oder einen NTP-Server.
Zeitsynchronisation mit NTP	Automatisches Stellen und periodischer Abgleich der Uhrzeit mittels eines NTP-Servers.
Zeitsynchronisation mit NTP (gesichert)	Automatisches Stellen und periodischer Abgleich der Uhrzeit mittels eines entsprechend konfigurierten NTP-Servers.

Tabelle 5- 2 Zeitsynchronisation für SCALANCE S $\geq$ V3.0

Auswahlmöglichkeit	Bedeutung / Auswirkung
Keine Zeitsynchronisation	Keine Zeitsynchronisation über den PC oder einen NTP-Server.
Zeit bei jedem Laden setzen	Automatisches Stellen der Modul-Uhrzeit mit der PC-Uhrzeit beim Laden einer Konfiguration.
Zeitsynchronisation mit NTP	Automatisches Stellen der Uhrzeit mittels eines NTP-Servers.

Modus zur Zeitsynchronisation auswählen

Gehen Sie folgendermaßen vor:

1. Wählen Sie den Synchronisierungsmodus aus.

2. Für SCALANCE S < V3.0: Bei der Synchronisierung durch einen NTP-Server geben Sie das Aktualisierungsintervall in Sekunden ein. Für SCALANCE S ≥ V3.0 wird das Zeitintervall für die Abfrage des NTP-Servers automatisch festgelegt.

Hinweis

CP

In STEP 7 angelegte NTP-Server werden automatisch mit dem Aktualisierungsintervall nach SCT migriert. Das Aktualisierungsintervall kann nur in STEP 7 geändert werden.

3. Weisen Sie dem Security-Modul über die Schaltfläche "Hinzufügen" einen bereits angelegten NTP-Server vom selben Typ zu, wie im Feld "Synchronisierungsmodus" ausgewählt.

Sind noch keine NTP-Server vorhanden, legen Sie über die Schaltfläche "NTP-Server..." einen NTP-Server an.

5.3.3 Eintrag hinzufügen

NTP-Server zur NTP-Liste hinzufügen

Klicken Sie auf die Schaltfläche "Hinzufügen...", um einen neuen Server anzulegen.

NTP-Server aus NTP-Liste bearbeiten

Klicken Sie auf die Schaltfläche "Eigenschaften...", um einen bestehenden Server zu bearbeiten.

Ergebnis: Der Dialog "Definition NTP-Server" wird geöffnet.

5.3.4 NTP-Server definieren

So definieren Sie einen neuen NTP-Server:

1. Geben Sie einen Namen für den NTP-Server ein.

Definition NTP-Server

Allgemeine Einstellungen

Name:

IP-Adresse:

Typ:

Schlüsselliste (nur bei NTP (gesichert))

Schlüssel-ID	Authentifizierung	Hex/ASCII	Schlüssel
1	SHA-1	ASCII	thisismykey1
2	SHA-1	ASCII	thisismykey2
3	MD5	ASCII	thisismykey3

Hinzufügen... Löschen Importieren... Exportieren...

OK Abbrechen Hilfe

2. Geben Sie die IP-Adresse des NTP-Servers ein.
3. Wählen Sie den Typ aus.

Einstellungen für NTP (gesichert)

CP

1. Klicken Sie auf die Schaltfläche "Hinzufügen".
2. Geben Sie die folgenden Daten ein:

Eigenschaft	Bedeutung
Schlüssel-ID	Numerischer Wert zwischen 1 ... 65534.
Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus aus.
Hex/ASCII	Wählen Sie das Format für den NTP-Schlüssel aus.
Schlüssel	Geben Sie den NTP-Schlüssel mit folgenden Längen ein: Hex: 22 ... 40 Zeichen ASCII: 11 ... 20 Zeichen
Löschen	Löschen Sie über die Schaltfläche den ausgewählten Eintrag.

Import / Export von NTP-Servern

Über die Schaltflächen "Import" bzw. "Export" können Sie die Schlüsselliste des aktuell angezeigten NTP-Servers exportieren und die Datei in einen NTP-Server importieren bzw. umgekehrt.

5.4 SNMP

5.4.1 Übersicht

Was ist SNMP?

Das Security-Modul unterstützt die Übertragung von Managementinformationen über das Simple Network Management Protocol (SNMP). Dafür ist auf dem Security-Modul ein "SNMP-Agent" installiert, der die SNMP-Anfragen entgegennimmt und beantwortet. Informationen über die Eigenschaften von SNMP-fähigen Geräten sind in sogenannten MIB-Dateien (Management Information Base) hinterlegt, für die der Benutzer die notwendigen Rechte haben muss.

Beim SNMPv1 wird der "Community String" mitgesendet. Der "Community String" ist wie ein Passwort, welches zusammen mit der SNMP-Anfrage verschickt wird. Ist der Community String korrekt, antwortet das Security-Modul mit der angeforderten Information. Ist der String falsch, verwirft das Security-Modul die Anfrage und antwortet nicht.

Bei SNMPv3 können die Daten verschlüsselt übertragen werden.

5.4.2 SNMP aktivieren



Voraussetzung

- Das Register "SNMP" wird nur angezeigt, wenn Sie den Erweiterten Modus eingeschaltet haben.

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.

Abhilfe SCT Standalone: Sie schließen das Projekt, ohne zu speichern und öffnen es erneut.

- STEP 7: Im Register "SNMP" ist das Kontrollkästchen "SNMP aktivieren" aktiviert.



So erreichen Sie diese Funktion

1. Markieren Sie das zu bearbeitende Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "SNMP".
3. Für SCALANCE S: Aktivieren Sie das Kontrollkästchen "SNMP aktivieren".
4. Wählen Sie eine der folgenden SNMP-Protokollversionen aus:

- SNMPv1

Das Security-Modul verwendet zur Steuerung der Zugriffsrechte im SNMP-Agent folgende Standardwerte für die Community Strings:

- Für Lesezugriff: public
- Für Lese- und Schreibzugriff: private

Hinweis**Standardwerte für Community Strings überschreiben**

Um die Sicherheit zu erhöhen, überschreiben Sie die Standardwerte der Community Strings mit neuen Namen.

Um den Schreibzugriff über SNMP zu aktivieren, wählen Sie die Option "Erlaube schreibenden Zugriff über Community String "private".

- SNMPv3

Wählen Sie entweder ein Authentifizierungsverfahren oder ein Authentifizierungs- und Verschlüsselungsverfahren aus.

- Authentifizierungs-Algorithmus: keine, MD5, SHA-1
- Verschlüsselungs-Algorithmus: keine, AES-128, DES

1. Weisen Sie dem Benutzer eine Rolle zu, bei der die entsprechenden SNMP-Rechte aktiviert sind. Eine Übersicht der SNMP-Rechte finden Sie in Kapitel Rechte verwalten (Seite 62).

5.5 Proxy-ARP

S≥V3.0

Übersicht

Proxy-ARP ermöglicht Routern, ARP-Anfragen für Hosts zu beantworten. Die Hosts befinden sich dabei in durch Router getrennten Netzen, verwenden jedoch den gleichen IP-Adressenbereich.

Sendet PC1 eine ARP-Anforderung an PC2, bekommt er von dem dazwischen liegenden Router und nicht von PC2 eine ARP-Antwort und die Hardwareadresse der Schnittstelle (MAC des Ports am Router), auf der die Anfrage empfangen wurde. Der anfragende PC1 sendet dann seine Daten an den Router, der sie dann an PC2 weiterleitet.

So erreichen Sie diese Funktion

Nur für internen Port und im Bridge-Modus.

1. Markieren Sie das zu bearbeitende Modul.

5.5 Proxy-ARP

2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "ARP-Proxy".
3. Wenn das Security-Modul eine ARP-Anfrage aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantworten soll, tragen Sie die entsprechende IP-Adresse ein.

Gesicherte Kommunikation im VPN über IPsec-Tunnel

6



In diesem Kapitel erfahren Sie, wie Sie die vom Security-Modul geschützten IP-Subnetze per Drag and Drop zu einem VPN (Virtual Private Network) verbinden.

Wie bereits im Kapitel zu den Moduleigenschaften beschrieben, können Sie es auch hier bei Standard-Einstellungen belassen, um eine sichere Kommunikation innerhalb Ihrer internen Netze zu betreiben.

Weitere Informationen



Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

Siehe auch

Online Funktionen - Test, Diagnose und Logging (Seite 203)

6.1 VPN mit Security-Modulen

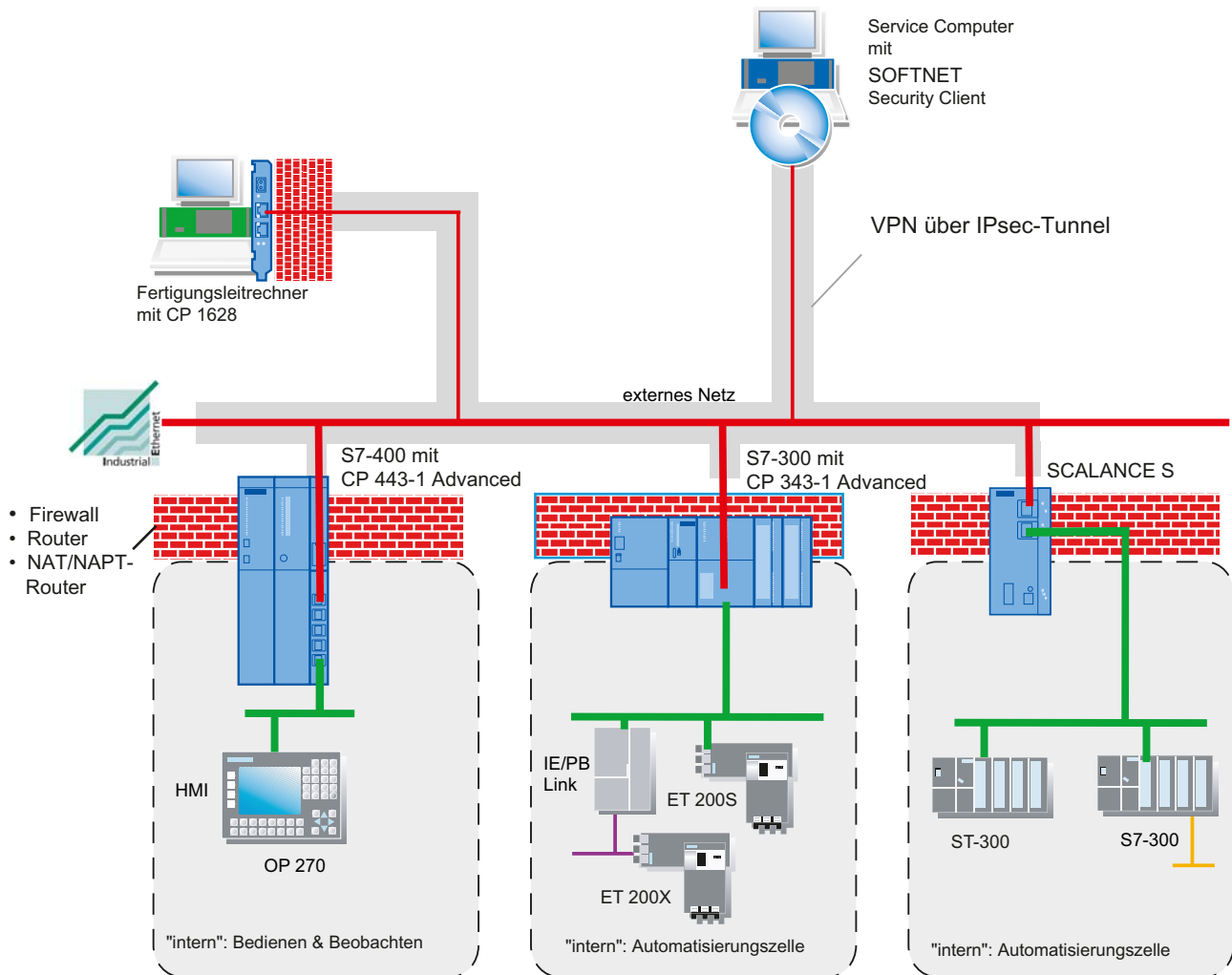
Sichere Verbindung durch ungeschütztes Netz

Für Security-Module, die das interne Netz schützen, stellen IPsec-Tunnel eine gesicherte Datenverbindung durch das unsichere externe Netz zur Verfügung.

Durch den Datenaustausch über IPsec werden für die Kommunikation die folgenden Sicherheitsaspekte realisiert:

- Vertraulichkeit
Stellt sicher, dass die Daten verschlüsselt übertragen werden.
- Integrität
Stellt sicher, dass die Daten nicht verändert worden sind.
- Authentizität
Stellt sicher, dass die VPN-Endpunkte auch vertrauenswürdig sind.

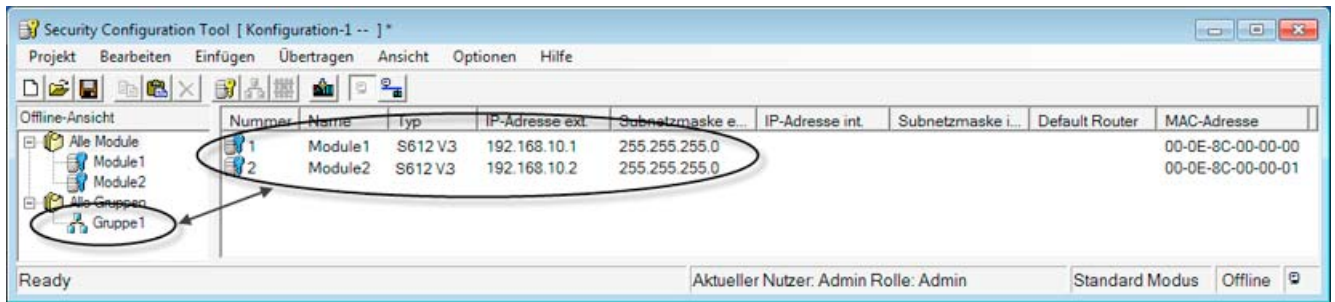
Das Security-Modul verwendet für die Tunnelung das IPsec-Protokoll (Tunnelmodus von IPsec).



Tunnelverbindungen bestehen zwischen Modulen der gleichen Gruppe (VPN)

Die Eigenschaften eines VPN werden bei den Security-Modulen innerhalb einer Modul-Gruppe für alle IPsec-Tunnel zusammengefasst.

IPsec-Tunnel werden automatisch zwischen allen Security-Modulen und SOFTNET Security Client-Modulen aufgebaut, die einer Gruppe angehören. Dabei kann ein Security-Modul in einem Projekt parallel mehreren verschiedenen Gruppen angehören.

**ACHTUNG**

Wird der Name eines Security-Moduls geändert, dann müssen alle Security-Module derjenigen Gruppen, denen das geänderte Security-Modul angehört, neu konfiguriert werden (Menübefehl "Übertragen" > "An alle Module...").

Wird der Name einer Gruppe geändert, dann müssen alle Security-Module dieser Gruppe neu konfiguriert werden (Menübefehl "Übertragen" > "An alle Module...").

ACHTUNG

Layer-2-Telegramme werden auch getunnelt, wenn sich zwischen zwei Security-Modulen ein Router befindet. Dazu müssen jedoch die MAC-Adressen der Kommunikationspartner statisch im Security Configuration Tool konfiguriert werden und gegebenenfalls statische ARP-Einträge auf den Kommunikationsgeräten eingetragen werden.

Allgemein gilt: Non-IP-Telegramme werden nur dann durch einen Tunnel übertragen, wenn die Geräte, die die Telegramme senden bzw. empfangen, auch schon vorher, d. h. ohne den Einsatz der Security-Module, kommunizieren konnten.

6.2 Authentifizierungsmethoden

Authentifizierungsmethoden

Die Authentifizierungsmethode wird innerhalb einer Gruppe (eines VPNs) festgelegt und bestimmt die Art der verwendeten Authentifizierung.

Es werden schlüsselbasierende oder zertifikatsbasierende Authentifizierungsmethoden unterstützt:

- Preshared Keys

Die Authentisierung erfolgt über eine zuvor verabredete Zeichenfolge, die an alle in der Gruppe befindlichen Module verteilt wird.

Geben Sie dafür im Dialog "Gruppeneigenschaften" im Feld "Preshared Key" ein Passwort ein.

- Zertifikat

Die zertifikatsbasierte Authentifizierung "Zertifikat" ist die Standardeinstellung, die auch im Standard Modus eingeschaltet ist. Das Verhalten ist wie folgt:

- Beim Anlegen einer Gruppe wird automatisch ein Gruppenzertifikat erzeugt (Gruppenzertifikat = CA-Zertifikat).
- Jedes Security-Modul, das in der Gruppe ist, erhält ein Zertifikat, das mit dem Schlüssel der Gruppen-CA signiert ist.

Sämtliche Zertifikate basieren auf dem ITU-Standard X.509v3 (ITU, International Telecommunications Union).

Die Zertifikate werden von einer im Security Configuration Tool enthaltenen Zertifizierungsstelle erzeugt.

ACHTUNG
Einschränkung bei VLAN-Betrieb
Bei IP-Telegrammen durch den VPN-Tunnel des Security-Moduls wird kein VLAN-Tagging übertragen. Die in den IP-Telegrammen enthaltenen VLAN-Tags gehen beim Passieren der Security-Module verloren, da für die Übertragung der IP-Telegramme IPsec verwendet wird.
Standardmäßig können mit IPsec keine IP-Broadcast- bzw. IP-Multicast-Telegramme durch einen Layer 3 VPN-Tunnel übertragen werden. Durch einen Layer 2 VPN-Tunnel des Security-Moduls werden IP-Broadcast- bzw. IP-Multicast-Telegramme genau wie MAC-Pakete inklusive Ethernet-Header in UDP "verpackt" und übertragen. Daher bleibt bei diesen Paketen das VLAN-Tagging erhalten.

6.3 VPN-Gruppen

6.3.1 Betriebsarten von VPN-Gruppen

VPN-Betriebsarten

Security-Module können gleichzeitig mehreren VPN-Gruppen und je nach Security-Modul auch unterschiedlichen Betriebsarten angehören.

Regeln für die Gruppenbildung

Beachten Sie die folgenden Regeln, wenn Sie VPN-Gruppen bilden wollen:

- Für SCALANCE S 612/613

Das erste in einer VPN-Gruppe zugeordnete Modul bestimmt, welche zusätzlichen Module hinzugefügt werden dürfen.

Ist das erste hinzugefügte SCALANCE S-Modul im Routing-Modus, so können zusätzlich nur SCALANCE S-Module mit aktiviertem Routing hinzugefügt werden. Ist das erste hinzugefügte SCALANCE S-Modul im Bridge-Modus, so dürfen zusätzlich nur SCALANCE S-Module im Bridge-Modus hinzugefügt werden. Soll der Modus einer VPN-Gruppe geändert werden, so müssen alle in der Gruppe enthaltenen Module entfernt und neu hinzugefügt werden. Ein CP kann in eine Gruppe mit einem SCALANCE S im Bridge- oder Routing-Modus hinzugefügt werden.

- Für CP und SCALANCE S 623

Wird ein CP oder SCALANCE S 623 als erstes Modul in eine VPN-Gruppe eingefügt, befindet sich die VPN-Gruppe im Bridge-Modus. Das nächste eingefügte Security-Modul bestimmt den Gruppenmodus. Befindet sich das Security-Modul im Routing-Modus, dürfen nur noch Security-Module eingefügt werden, die sich auch im Routing-Modus befinden.

Ein CP oder SCALANCE S 623 kann gleichzeitig mehreren VPN-Gruppen mit unterschiedlicher Betriebsart zugeordnet werden. Der CP oder das SCALANCE S 623 wird dann im Mischbetrieb betrieben.

- Es ist nicht möglich, ein SCALANCE M-Modul einer VPN-Gruppe hinzuzufügen, die ein Modul im Bridge-Modus enthält.

Entnehmen Sie der folgenden Tabelle, welche Module zusammen in einer VPN-Gruppe zusammengefasst werden können:

Tabelle 6- 1 Security-Module und VPN-Betriebsarten

Modul	Kann aufgenommen werden in VPN-Gruppe im...		
	Bridge-Modus	Routing-Modus	Mischbetrieb
SCALANCE S 612/613 im Bridge-Modus	x	-	-
SCALANCE S 612/613 im Routing-Modus	-	x	-
SCALANCE S 623 im Bridge-Modus	x	x	x
SCALANCE S 623 im Routing-Modus	x	x	x
CP x43 Adv.	x	x	x
CP 1628	x	x	x
SOFTNET Security Client 2005	x	-	-
SOFTNET Security Client 2008	x	x	-
SOFTNET Security Client V3.0	x	x	-
SOFTNET Security Client V4.0	x	x	x
SCALANCE M	-	x	-

6.3.2 Gruppen anlegen und Module zuordnen

Voraussetzung

ACHTUNG

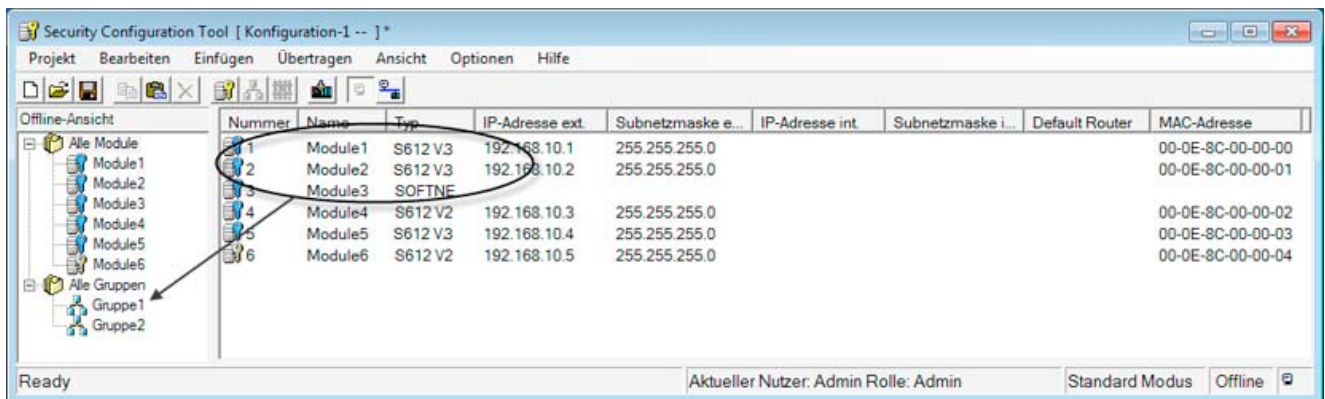
Aktuelles Datum und aktuelle Uhrzeit auf den Security-Modulen

Achten Sie bei der Verwendung von gesicherter Kommunikation (z. B. HTTPS, VPN...) darauf, dass die betroffenen Security-Module über die aktuelle Uhrzeit und das aktuelle Datum verfügen. Die verwendeten Zertifikate werden sonst als nicht gültig ausgewertet und die gesicherte Kommunikation funktioniert nicht.

So erreichen Sie diese Funktion

1. Legen Sie über den Menübefehl "Einfügen" > "Gruppe" eine Gruppe an.

- Ordnen Sie der Gruppe die Security-Module und SOFTNET Security Client-Module zu, die zu einer VPN-Gruppe gehören sollen. Ziehen Sie hierzu mit der Maus das Modul auf die gewünschte Gruppe (Drag and Drop).



Eigenschaften projektieren

Wie bei der Konfiguration von Modulen wirken sich auch bei der Konfiguration von Gruppen die beiden wählbaren Bedienungssichten im Security Configuration Tool aus:

- Standard Modus**

Im Standard Modus belassen Sie es bei den vom System vergebenen Voreinstellungen. Auch als Nicht-IT-Experten können Sie so IPsec-Tunnel konfigurieren und eine sichere Datenkommunikation in Ihren internen Netzen betreiben.

- Erweiterter Modus**

Der Erweiterte Modus bietet Ihnen Einstellmöglichkeiten zur spezifischen Konfiguration der Tunnelkommunikation.

Hinweis

Parametrierung von SCALANCE M bzw. anderer VPN-Clients

Zur Parametrierung vom SCALANCE M bzw. anderer VPN-Clients müssen sie modulspezifische VPN-Eigenschaften im Erweiterten Modus konfigurieren.

Alle projektierten Gruppen mit ihren Eigenschaften anzeigen

- Selektieren Sie im Navigationsbereich das Objekt "VPN-Gruppen".

Folgende Eigenschaften der Gruppen werden spaltenweise angezeigt:

Eigenschaft/Spalte	Bedeutung	Kommentar/Auswahl
Gruppenname	Gruppenname	frei wählbar
Authentifizierung	Authentifizierungstyp	- Preshared Key - Zertifikat

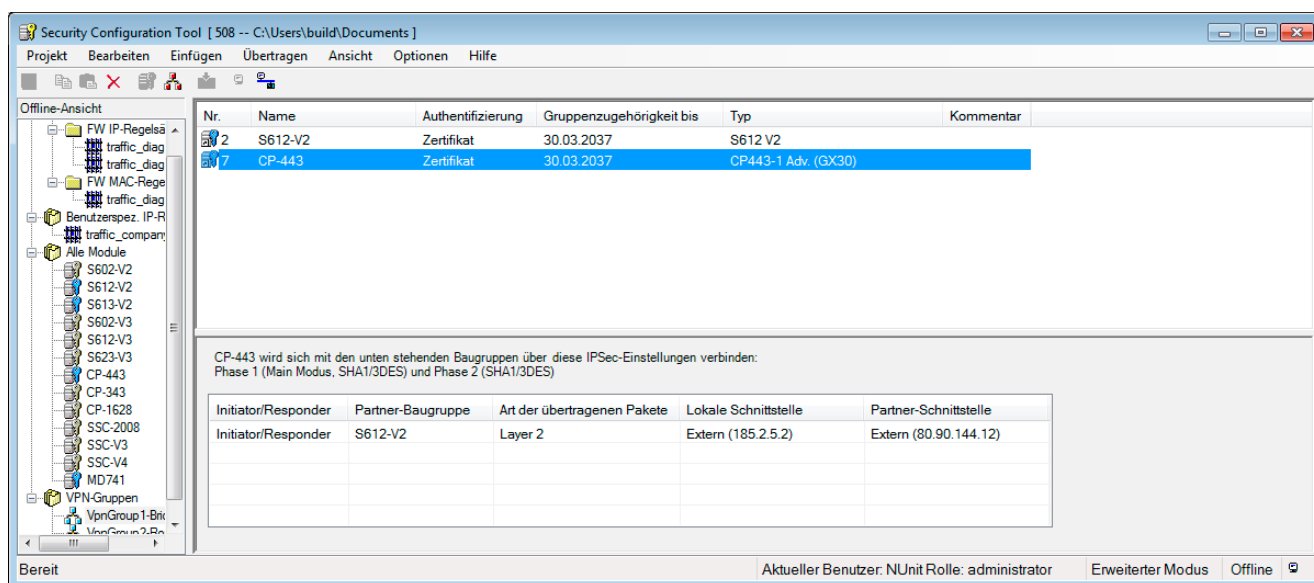
Eigenschaft/Spalte	Bedeutung	Kommentar/Auswahl
Gruppenzugehörigkeit bis...	Lebensdauer von Zertifikaten	siehe Abschnitt "Lebensdauer von Zertifikaten einstellen"
Kommentar	Kommentar	frei wählbar

VPN-Verbindungsdetails anzeigen und konfigurieren

1. Markieren Sie im Navigationsbereich die zu bearbeitende VPN-Gruppe.
2. Klicken Sie im Inhaltsbereich auf ein Modul.

Ergebnis: Im Vorschaubereich werden die anderen VPN-Gruppenteilnehmer, zu denen das selektierte Modul je eine VPN-Verbindung aufbaut, angezeigt.

3. Wählen Sie aus, über welche Schnittstelle die VPN-Gruppenteilnehmer kommunizieren sollen.



Lebensdauer von Zertifikaten einstellen

Öffnen Sie den Dialog, in dem Sie das Ablaufdatum des Zertifikats eingeben können, wie folgt:

1. Markieren Sie im Navigationsbereich die zu bearbeitende VPN-Gruppe.
2. Wählen Sie über die rechte Maustaste den Menübefehl "Eigenschaften".

Hinweis

Ablauf eines Zertifikats

Die Kommunikation durch den VPN-Tunnel läuft nach Ablauf des Zertifikats weiter, bis der Tunnel abgebaut wird oder die SA-Lebensdauer abläuft. Weitere Informationen zu Zertifikaten finden Sie im Kapitel Zertifikate verwalten (Seite 66).

6.4 Tunnelkonfiguration im Standard Modus

Gruppeneigenschaften

Im Standard Modus gelten folgende Eigenschaften:

- Alle Parameter der IPsec-Tunnel und die Authentifizierungsmethode sind fest vorgegeben.

Im Eigenschaftendialog für die Gruppe können Sie die eingestellten Standardwerte anzeigen.

- Der Lernmodus ist für alle Module aktiviert.

Dialog zur Anzeige der Standardwerte öffnen

1. Markieren Sie die Gruppe.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...".

Die Anzeige ist identisch zum Dialog im Erweiterten Modus, jedoch können Sie die Werte nicht verändern.

6.5 Tunnelkonfiguration im Erweiterten Modus

Der Erweiterte Modus bietet Ihnen Einstellmöglichkeiten zur spezifischen Konfiguration der Tunnelkommunikation.

In den Erweiterten Modus umschalten

Schalten Sie für alle in diesem Kapitel beschriebenen Funktionen den Erweiterten Modus ein.

Hinweis

Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.

Abhilfe SCT Standalone: Sie schließen das Projekt ohne zu speichern und öffnen es erneut.

6.5.1 Gruppeneigenschaften projektieren

Gruppeneigenschaften

ACHTUNG
IPsec-Kenntnisse erforderlich Um diese Parameter einstellen zu können, benötigen Sie IPsec-Kenntnisse. Wenn Sie keine Einstellungen vornehmen bzw. verändern, gelten die Standardeinstellungen des Standard Modus.

Im Erweiterten Modus sind folgende Gruppeneigenschaften einstellbar:

- Authentifizierungsmethode
- IKE-Einstellungen (Dialogbereich: Erweiterte Einstellungen Phase 1)
- IPsec-Einstellungen (Dialogbereich: Erweiterte Einstellungen Phase 2)

So erreichen Sie diese Funktion

1. Markieren Sie im Navigationsbereich die zu bearbeitende VPN-Gruppe.

2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...".

Gruppeneigenschaften - VpnGroup1-Bridge

☐ Preshared Key

Schlüssel: CKjWoJGC1Qx6yAUQ

☒ Zertifikat

Name: P5DB1-G103A

Neues Eigenschaften...

Erweiterte Einstellungen Phase 1

IKE-Modus: Main

Phase 1 DH-Gruppe: Group2

SA-Lebensdauertyp: Time SA-Lebensdauer: 2500000 Min.

Phase 1 Verschlüsselung: 3DES-168 Phase 1 Authentifizierung: SHA1

Erweiterte Einstellungen Phase 2

SA-Lebensdauertyp: Time SA-Lebensdauer: 2880 Min.

Phase 2 Verschlüsselung: 3DES-168 Phase 2 Authentifizierung: SHA1

☐ Perfect Forward Secrecy

Kommentar

OK Abbrechen Hilfe

3. Wählen Sie aus, ob für die Authentifizierung ein Preshared Key oder Zertifikat verwendet werden soll. Weitere Informationen hierzu finden Sie im Kapitel Authentifizierungsmethoden (Seite 164).

Parameter für erweiterte Einstellungen Phase 1 - IKE-Einstellungen

Phase 1: Schlüsselaustausch (IKE = Internet Key Exchange):

Stellen Sie hier die Parameter für das Protokoll des IPsec-Schlüsselmanagements ein. Der Schlüsselaustausch erfolgt über das standardisierte Verfahren IKE, für das Sie folgende Protokollparameter einstellen können:

Parameter	Beschreibung
IKE-Modus	Schlüsselaustauschverfahren: • Main Mode • Aggressive Mode Der Unterschied zwischen Main- und Aggressive Mode ist die "Identity-Protection", die im Main-Mode verwendet wird. Die Identität wird im Main-Mode verschlüsselt übertragen, im Aggressive-Mode nicht.
Phase 1 DH-Gruppe	Diffie-Hellman-Schlüsselvereinbarung: • Group 1 • Group 2 • Group 5 Diffie-Hellman-Gruppen (wählbare kryptographische Algorithmen im Oakley-Schlüsselaustausch-Protokoll).
SA-Lebensdauertyp	Phase 1 Security Association (SA): • Time: Zeitbegrenzung in Minuten Die Nutzdauer für das aktuelle Schlüsselmaterial wird zeitlich begrenzt. Nach Ablauf der Zeit wird das Schlüsselmaterial neu ausgehandelt.
SA-Lebensdauer	Numerischer Wert: Wertebereich für Time: 1440 ... 2500000 Minuten (Standard: 2500000)
Phase 1 Verschlüsselung	Verschlüsselungs-Algorithmus: • DES: Data Encryption Standard (56 Bit Schlüssellänge, Modus CBC) • 3DES-168: Dreifach-DES (168 Bit Schlüssellänge, Modus CBC) • AES-128, 192, 256: Advanced Encryption Standard (128, 192 Bit oder 256 Bit Schlüssellänge, Modus CBC)
Phase 1 Authentifizierung	Authentisierungs-Algorithmus: • MD5: Message Digest Algorithm 5 • SHA1: Secure Hash Algorithm 1

Parameter für erweiterte Einstellungen Phase 2 - IPsec-Einstellungen

Phase 2: Datenaustausch (ESP = Encapsulating Security Payload)

Stellen Sie hier die Parameter für das Protokoll des IPsec-Datenaustauschs ein. Der Datenaustausch erfolgt im "Quick Mode". Die gesamte Kommunikation in dieser Phase erfolgt verschlüsselt über das standardisierte Sicherheitsprotokoll ESP, für das Sie folgende Protokollparameter einstellen können:

Parameter	Beschreibung
SA-Lebensdauertyp	Phase 2 Security Association (SA): - Time: Zeitbegrenzung in Minuten Die Nutzdauer für das aktuelle Schlüsselmaterial wird zeitlich begrenzt. Nach Ablauf der Zeit wird das Schlüsselmaterial neu ausgehandelt. - Limit: Begrenzung des Datenvolumen in Mbyte
SA-Lebensdauer	Numerischer Wert: - Wertebereich für Time: 60 ... 16666666 Minuten (Standard: 2880) - Wertebereich für Limit: 2000 ... 500000 Mbyte (Standard: 4000)
Phase 2 Verschlüsselung	Verschlüsselungs-Algorithmus: - DES: Data Encryption Standard (56 Bit Schlüssellänge, Modus CBC) 3DES-168: Dreifach-DES (168 Bit Schlüssellänge, Modus CBC) - AES-128: Advanced Encryption Standard (128 Bit Schlüssellänge, Modus CBC)
Phase 2 Authentifizierung	Authentisierungs-Algorithmus: - MD5: Message Digest Algorithm 5 - SHA1: Secure Hash Algorithm 1
Perfect Forward Secrecy	Wählen Sie aus, ob vor jedem neuen Aushandeln einer IPsec-SA ein erneutes Aushandeln der Schlüssel mit Hilfe des Diffie-Hellman-Verfahrens erfolgen soll. Durch das Perfect Forward Secrecy wird sicher gestellt, dass von den zuvor generierten Schlüsseln nicht auf die neuen Schlüssel geschlossen werden kann.

6.5.2 Security-Modul in konfigurierte Gruppe aufnehmen

Die projektierten Gruppeneigenschaften werden für Security-Module, die in eine bestehende Gruppe aufgenommen werden, übernommen.

So gehen Sie vor

Je nachdem, ob Sie an den Gruppeneigenschaften etwas geändert haben oder nicht, müssen Sie beim Vorgehen unterscheiden:

- **Fall a:** Wenn Sie die Gruppeneigenschaften nicht geändert haben

1. Fügen Sie die neuen Security-Module der Gruppe hinzu.
2. Laden Sie die Konfiguration in die neuen Module.

- **Fall b:** Wenn Sie die Gruppeneigenschaften geändert haben

1. Fügen Sie die neuen Security-Module der Gruppe hinzu.
2. Laden Sie die Konfiguration in alle Module, die zur Gruppe gehören.

Vorteil

Bereits vorhandene, in Betrieb genommene Security-Module müssen nicht neu projiziert und geladen werden. Die laufende Kommunikation wird nicht beeinflusst oder unterbrochen.

Einstellungen für Teilnehmer mit unbekannter IP-Adresse

Teilnehmer, bei denen zum Projektierungszeitpunkt die IP-Adresse unbekannt ist (Unknown Peers), können in eine bestehende VPN-Gruppe eingefügt werden. Da sich die Teilnehmer meist im mobilen Einsatz befinden und die IP-Adresse dynamisch beziehen (z. B. ein SOFTNET Security Client oder SCALANCE M), kann der VPN-Tunnel nur aufgebaut werden, wenn Sie die Parametereinstellungen für Phase 1 entsprechend einer der folgenden Tabellen vornehmen. Verwenden Sie andere Einstellungen, können Sie keinen VPN-Tunnel zum Endgerät aufbauen.

Tabelle 6- 2 Verschlüsselungsparameter 1

Parameter	Einstellung
Phase 1 Verschlüsselung	AES-256
Phase 1 DH-Gruppe	Group2
Phase 1 Authentifizierung	SHA1
Authentifizierungsmethode	Zertifikat
SA-Lebensdauer	1 ... 2500000 Minuten

Tabelle 6- 3 Verschlüsselungsparameter 2

Parameter	Einstellung
Phase 1 Verschlüsselung	3DES-168
Phase 1 DH-Gruppe	Group2
Phase 1 Authentifizierung	SHA1
Authentifizierungsmethode	Zertifikat
SA-Lebensdauer	1 ... 2500000 Minuten

Tabelle 6- 4 Verschlüsselungsparameter 3

Parameter	Einstellung
Phase 1 Verschlüsselung	DES
Phase 1 DH-Gruppe	Group2
Phase 1 Authentifizierung	MD5
Authentifizierungsmethode	Zertifikat
SA-Lebensdauer	1 ... 2500000 Minuten

Tabelle 6- 5 Verschlüsselungsparameter 4

Parameter	Einstellung
Phase 1 Verschlüsselung	3DES-168
Phase 1 DH-Gruppe	Group2
Phase 1 Authentifizierung	SHA1
Authentifizierungsmethode	Preshared Key
SA-Lebensdauer	1 ... 2500000 Minuten

Zusätzliche Einschränkungen für den SOFTNET Security Client

Für den SOFTNET Security Client gelten zusätzlich die folgenden Einschränkungen:

Parameter	Einstellung / Besonderheit
Phase 1 Verschlüsselung	AES-256 nur bei Windows 7 möglich
Phase 1 SA-Lebensdauer	1440 ... 2879 Minuten
SA-Lebensdauertyp	Muss für beide Phasen identisch gewählt werden
Phase 2 Verschlüsselung	Kein AES-128 möglich
Phase 2 SA-Lebensdauer	1440 ... 2879 Minuten
Phase 2 Authentifizierung	Kein MD5 möglich

Aktive Teilnehmer in eine VPN-Gruppe aufnehmen

Wird ein aktiver Teilnehmer in eine bestehende VPN-Gruppe hinzugefügt, so kann dieser die Gruppenteilnehmer erreichen, ohne dass Sie das Projekt erneut auf alle Teilnehmer der VPN-Gruppe laden.

ACHTUNG
Wenn Sie einen aktiven Teilnehmer aus einer bestehenden VPN-Gruppe entfernen, kann dieser immer noch eine Verbindung zu den Gruppenteilnehmern aufbauen, auch wenn Sie das Projekt erneut auf alle Teilnehmer der VPN-Gruppe geladen haben. Soll der entfernte aktive Teilnehmer keine Verbindung mehr aufbauen können, erneuern Sie das CA-Gruppenzertifikat und laden Sie das Projekt erneut auf die Teilnehmer der VPN-Gruppe. Erneuert werden kann das Zertifikat in den Gruppeneigenschaften der VPN-Gruppe oder im Zertifikatsmanager, Register "Zertifizierungsstellen".

6.5.3 Modulspezifische VPN-Eigenschaften konfigurieren

Bedeutung

Für den Datenaustausch über die IPsec-Tunnel im VPN können Sie folgende modulspezifische Eigenschaften konfigurieren:

- Dead-Peer-Detection
- Erlaubnis zur Initiierung des Verbindungsaufbaus
- Öffentliche IP-Adresse zur Kommunikation über Internet-Gateways

Voraussetzung

Im Register "VPN" können Sie nur Einstellungen vornehmen, wenn sich das zu konfigurierende Security-Modul in einer VPN-Gruppe befindet.

So erreichen Sie diese Funktion

1. Markieren Sie das zu bearbeitende Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "VPN".

Dead-Peer-Detection (DPD)

Standardmäßig ist DPD aktiviert.

Bei aktivierter DPD tauschen die Module in einstellbaren Zeitintervallen zusätzliche Nachrichten aus. Hierdurch kann erkannt werden, ob die IPsec-Verbindung noch gültig ist oder eventuell neu aufgebaut werden muss. Besteht keine Verbindung mehr, werden die "Security Associations" (SA) von Phase 2 vorzeitig beendet. Bei deaktivierter DPD wird die SA erst nach Ablauf der SA-Lebensdauer beendet. Zur Einstellung der SA-Lebensdauer siehe Konfiguration der Gruppeneigenschaften.

Erlaubnis zur Initiierung des Verbindungsaufbaus

Sie können die Erlaubnis zur Initiierung des VPN-Verbindungsaufbaus auf bestimmte Module im VPN beschränken.

Maßgebend für die Einstellung des beschriebenen Parameters ist die Vergabe der IP-Adresse für das Gateway des zu projektierenden Moduls. Bei einer statisch vergebenen IP-Adresse kann das Modul von der Gegenstelle gefunden werden. Bei dynamisch vergebener, und daher sich ständig ändernder IP-Adresse, kann die Gegenstelle nicht ohne Weiteres eine Verbindung aufbauen.

Modus	Bedeutung
Starte Verbindung zur Gegenstelle (Standard)	Bei dieser Option ist das Modul "aktiv", d. h. es versucht, mit einer festen IP-Adresse eine Verbindung zur Gegenstelle herzustellen. Diese Option wird empfohlen, wenn Sie von dem Provider für das Gateway des hier zu projektierenden Security-Moduls eine dynamische IP-Adresse zugewiesen bekommen haben. Die Adressierung der Gegenstelle erfolgt über deren projektierte WAN-IP-Adresse oder deren externe Modul IP-Adresse.
Warte auf Gegenstelle	Bei dieser Option ist das Modul "passiv", d. h. es wartet, bis der Verbindungsaufbau von der Gegenstelle initiiert wird. Diese Option wird empfohlen, wenn Sie von dem Provider für das Gateway des hier zu projektierenden Security-Moduls eine statische IP-Adresse zugewiesen bekommen haben. Sie erreichen dadurch, dass Verbindungsaufbauversuche nur durch die Gegenstelle mit dynamischer WAN-IP-Adresse gestartet werden.

ACHTUNG

Stellen Sie nicht alle Module einer VPN-Gruppe auf "Warte auf Gegenstelle", da sonst keine Verbindung aufgebaut wird.

WAN-IP-Adresse - IP-Adressen der Module und Gateways bei einem VPN über Internet

Beim Betrieb eines VPN mit IPsec-Tunnel über das Internet sind in der Regel zusätzliche IP-Adressen für die Internet-Gateways, z. B. DSL-Router, erforderlich. Den einzelnen Security- oder SCALANCE M-Modulen müssen die externen IP-Adressen der Partner-Module im VPN bekannt sein.

Hinweis

Für die Nutzung eines WAN als externes, öffentliches Netzwerk geben Sie als "IP-Adresse ext." Ihre vom Provider erhaltene IP-Adresse an, über welche das Security-Modul dann im WAN (Internet) erreichbar ist. Damit das Security-Modul Pakete über das WAN (Internet) versenden kann, müssen Sie als "Standard-Router" Ihren DSL-Router eintragen.

Wenn Sie einen DSL-Router als Internet-Gateway nutzen, müssen an diesem mindestens die folgenden Ports freigeschaltet werden:

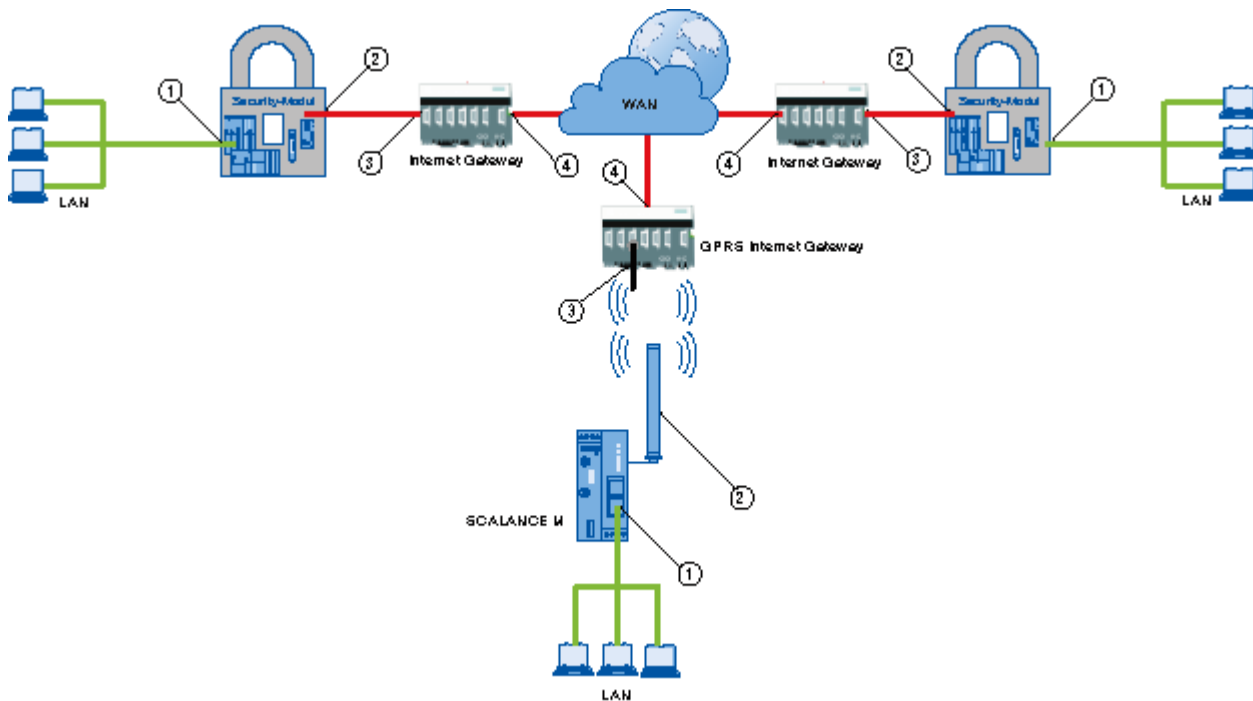
- Port 500 (ISAKMP)
- Port 4500 (NAT-T)

Für SCALANCE S muss bei Konfigurations-Downloads (über das WAN ohne aktiven Tunnel) zusätzlich der Port 443 (HTTPS) freigeschaltet werden.

Hierzu besteht die Möglichkeit, in der Konfiguration des Moduls eine externe IP-Adresse als "WAN-IP-Adresse" zuzuordnen. Beim Laden der Modulkonfiguration werden den Gruppenteilnehmern dann die WAN-IP-Adressen der Partner-Module mitgeteilt.

Ob die externe IP-Adresse oder WAN-IP-Adresse verwendet werden soll, können Sie auswählen, indem Sie innerhalb einer VPN-Gruppe auf das entsprechende Security-Modul klicken und im Inhaltsbereich die Adresse auswählen. Weitere Informationen hierzu finden Sie in Kapitel Gruppen anlegen und Module zuordnen (Seite 166).

Tragen Sie keine WAN-IP-Adresse ein, wird die externe IP-Adresse des Moduls verwendet.



- ① IP-Adresse intern - eines Moduls
- ② IP-Adresse extern - eines Moduls
- ③ IP-Adresse intern - eines Internet Gateways (z. B. GPRS-Gateway)
- ④ IP-Adresse extern (WAN-IP-Adresse) - eines Internet Gateways (z. B. DSL-Router)

6.6 Interne Netzknoten konfigurieren

Interne Netzknoten konfigurieren

Jedem Security-Modul müssen die Netzknoten im gesamten internen Netz bekannt sein, um die Authentizität eines Telegramms feststellen zu können.

Das Security-Modul muss sowohl seine eigenen internen Knoten kennen als auch die internen Knoten der Security-Module, mit denen es zusammen in einer VPN-Gruppe ist. Diese Information wird auf einem Security-Modul dazu verwendet zu bestimmen, welches Datenpaket in welchem Tunnel übertragen werden soll.

SCA.

Das Security-Modul bietet die Möglichkeit, die Netzknoten automatisch zu erlernen oder statisch zu konfigurieren.

Knoten bei Security-Modulen im Bridge-Modus

- SCALANCE S

Für ein SCALANCE S im Bridge-Modus können Sie hier die statischen internen Subnetze sowie die internen IP/MAC-Knoten konfigurieren und das automatisch Lernen interner Knoten zulassen oder sperren.

- CP 1628

Sie können die statischen NDIS-Knoten konfigurieren, indem Sie die durch den VPN-Tunnel erreichbaren NDIS-Knoten eintragen. Das automatische Lernen interner Knoten ist immer aktiviert.

Security-Modul im Routing-Modus und Teilnehmer einer VPN-Gruppe

- SCALANCE S

Tragen Sie die internen Teilnehmer / komplette Subnetze ein, die durch den VPN-Tunnel erreicht werden sollen.

Im Routing-Modus werden komplette Subnetze getunnelt; dort ist das Lernen der Netzknoten nicht notwendig.

- CP x43-1 Adv.

Wählen Sie aus, zu welchen Subnetzen des CP die VPN-Verbindungspartner, welche sich in Routing Beziehung zu dem CP befinden (SCALANCE S im Routing Modus und SCALANCE M), Zugriff haben dürfen.

6.6.1 Arbeitsweise des Lernmodus

Teilnehmer für die Tunnelkommunikation automatisch finden (bei SCALANCE S nur Bridge-Modus)

Ein großer Vorteil für die Konfiguration und den Betrieb der Tunnelkommunikation ist, dass Security-Module die Teilnehmer im internen Netzen selbsttätig auffinden können.

Neue Teilnehmer werden vom Security-Modul im laufenden Betrieb erkannt. Die erkannten Teilnehmer werden an die Security-Module gemeldet, die zur selben Gruppe gehören. Dadurch ist der Datenaustausch innerhalb der Tunnel einer Gruppe jederzeit in beide Richtungen gewährleistet.

Voraussetzungen

Erkannt werden folgende Teilnehmer:

- IP-fähige Netzknoten

IP-fähige Netzknoten werden gefunden, wenn Sie eine ICMP-Antwort auf den ICMP-Subnetz-Broadcast senden.

IP-Knoten hinter Routern sind auffindbar, wenn die Router ICMP-Broadcasts weiterleiten.

- ISO-Netzknoten

Netzknoten, die zwar nicht IP-fähig sind, jedoch über ISO-Protokolle ansprechbar sind, können ebenfalls gelernt werden.

Voraussetzung ist, dass sie auf XID- bzw. TEST-Telegramme antworten. TEST und XID (Exchange Identification) sind Hilfsprotokolle zum Informationsaustausch auf der Layer 2-Ebene. Durch das Versenden dieser Telegramme mit einer Broadcast-Adresse können diese Netzknoten ausfindig gemacht werden.

- PROFINET-Knoten

Mit Hilfe von DCP (Discovery and basic Configuration Protocol) werden PROFINET-Knoten gefunden.

Netzknoten, die diese Bedingungen nicht erfüllen, müssen Sie manuell konfigurieren.

Subnetze

Konfiguriert werden müssen auch Subnetze, die sich hinter internen Routern befinden.

Lernmodus ein-/ausschalten

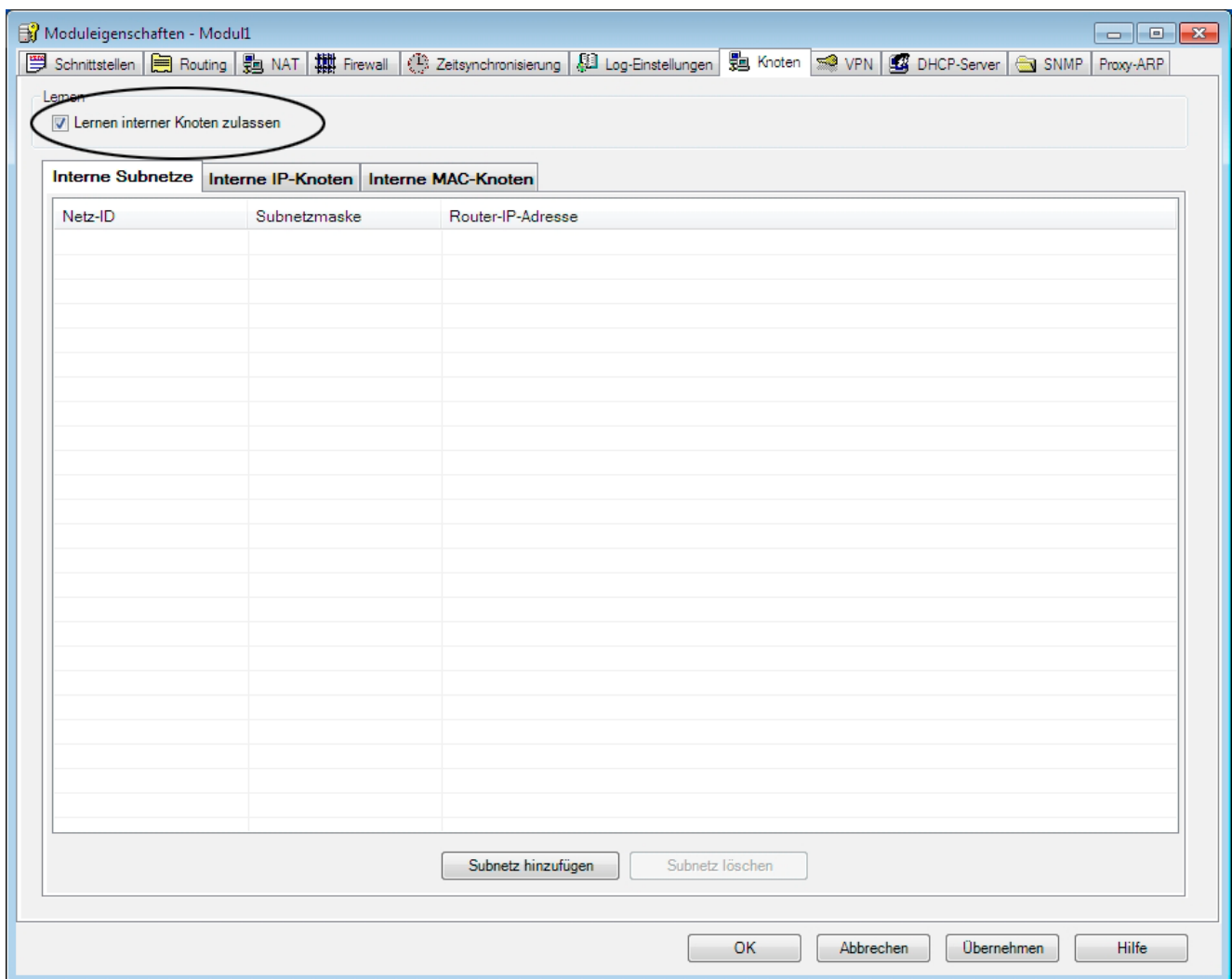
Die Lernfunktion ist in der Konfiguration durch die Projektierungssoftware Security Configuration Tool standardmäßig für jedes Security-Modul eingeschaltet.

Das Lernen kann für SCALANCE S auch völlig abgeschaltet werden. Dann müssen Sie alle internen Netzknoten, die an der Tunnelkommunikation teilnehmen sollen, manuell konfigurieren.

So erreichen Sie die Funktion

SCA.

1. Markieren Sie das Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Knoten".



Wann ist es sinnvoll, den automatischen Lernmodus auszuschalten?

Die Standardeinstellungen für das Security-Modul gehen davon aus, dass interne Netze stets sicher sind; das heißt auch, dass im Normalfall keine Netzknoten in das interne Netz zugeschaltet werden, die nicht vertrauenswürdig sind.

Das Ausschalten des Lernmodus kann sinnvoll sein, wenn das interne Netz statisch ist, d. h., wenn sich die Anzahl der internen Knoten und deren Adressen sich nicht ändern.

Mit Ausschalten des Lernmodus entfällt im internen Netz die Belastung des Mediums und der Knoten durch die Lerntelegramme. Auch das Security-Modul wird etwas leistungsfähiger, da es nicht durch die Bearbeitung der Lerntelegramme belastet wird.

6.6 Interne Netzknoten konfigurieren

Anmerkung: Im Lernmodus werden alle Knoten im internen Netz erfasst. Die Angaben zum VPN-Mengengerüst beziehen sich nur auf die Knoten, die im internen Netz über VPN kommunizieren.

ACHTUNG

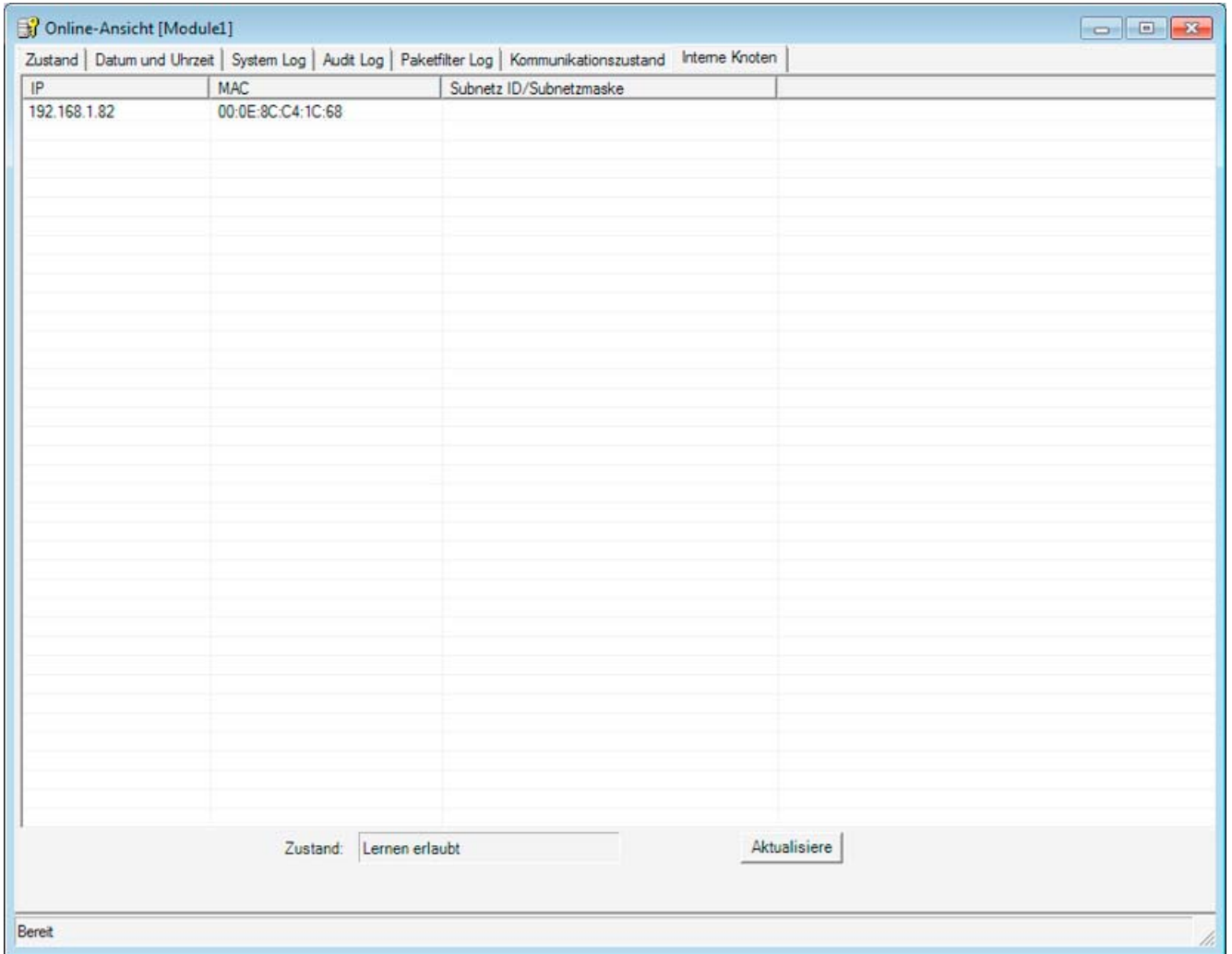
Werden im internen Netz mehr als 128 interne Knoten betrieben, wird damit das zulässige Mengengerüst überschritten und ein nicht erlaubter Betriebszustand erzeugt. Aufgrund der Dynamik im Netzwerkverkehr kommt es dann dazu, dass interne Knoten, die bereits gelernt wurden, wieder durch neue, bis jetzt noch nicht bekannte interne Knoten ersetzt werden.
--

6.6.2 Anzeige der gefundenen internen Netzknoten

Alle gefundenen Netzknoten werden im Security Configuration Tool angezeigt.

1. Wechseln Sie in die Betriebsart "Online".

2. Wählen Sie den Menübefehl "Bearbeiten" > "Online Diagnose...", Register "Interne Knoten".



Nicht-lernbare Netzknoten

Es gibt Teilnehmer im internen Netz, die nicht gelernt werden können. Diese Teilnehmer müssen Sie im Erweiterten Modus konfigurieren.

Sie müssen auch Subnetze konfigurieren, die sich im internen Netz des Security-Moduls befinden.

So erreichen Sie dieses Register

1. Markieren Sie das Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Knoten".
3. Geben Sie in den einzelnen Registern die erforderlichen Adressparameter zu allen Netzknoten an, die vom gewählten Security-Modul geschützt werden sollen.

Auswirkung beim Einsatz des SOFTNET Security Client

Wenn Sie Teilnehmer statisch konfigurieren, müssen Sie auch die Konfiguration für einen in der VPN-Gruppe genutzten SOFTNET Security Client neu laden.

Je nach Security-Modul und Modus stehen Ihnen verschiedene Register zur Auswahl, die in der Online-Hilfe beschrieben werden.

SOFTNET Security Client

Mit der PC-Software SOFTNET Security Client sind gesicherte Fernzugriffe vom PC/PG auf Automatisierungsgeräte, die durch Security-Module geschützt sind, über öffentliche Netze hinweg möglich.

In diesem Kapitel wird beschrieben, wie Sie den SOFTNET Security Client im Security Configuration Tool projektieren und anschließend auf dem PC/PG in Betrieb nehmen.

Weitere Informationen



Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe des SOFTNET Security Client.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

Siehe auch

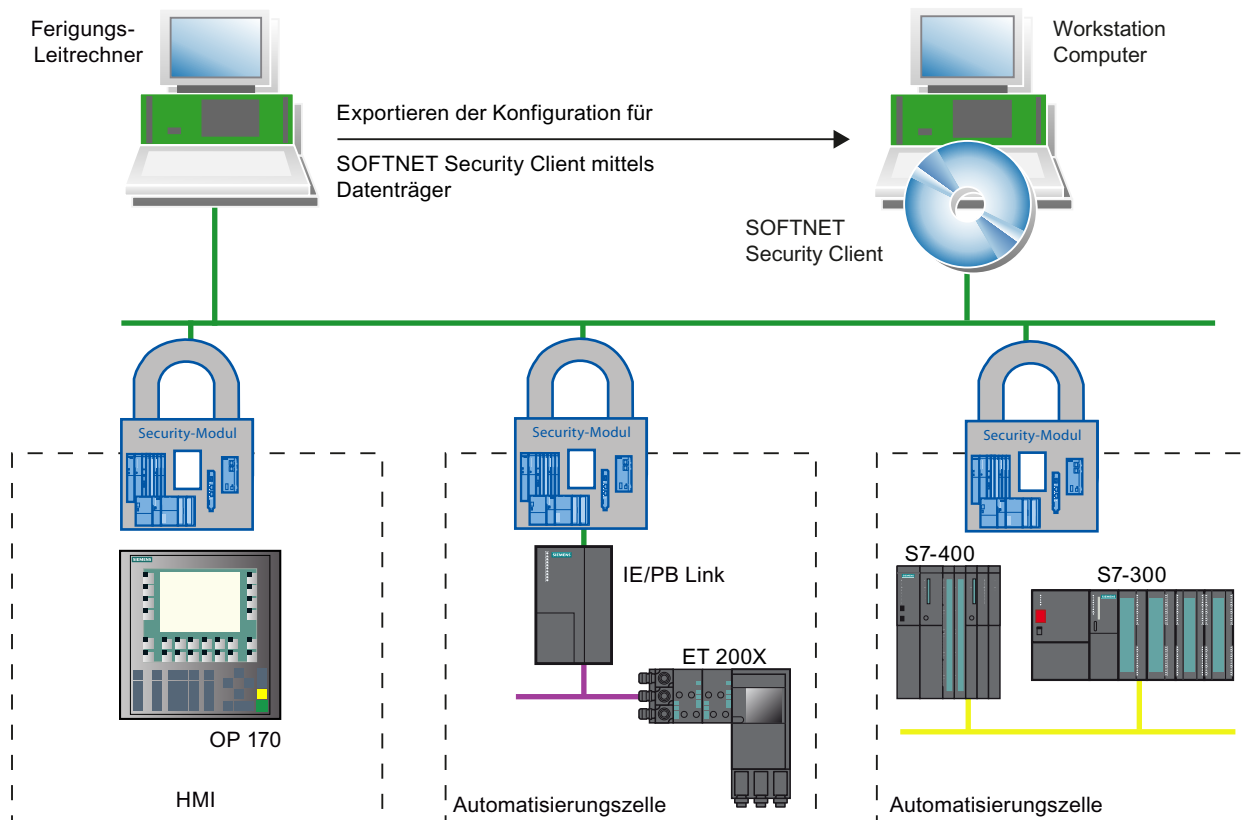
Gesicherte Kommunikation im VPN über IPsec-Tunnel (Seite 161)

7.1 Einsatz des SOFTNET Security Client

Einsatzbereich - Zugriff über VPN

Mit dem SOFTNET Security Client konfigurieren Sie einen PC/PG so, dass er automatisch eine gesicherte IPsec-Tunnelverbindung im VPN (Virtual Private Network) zu einem oder mehreren Security-Modulen aufbauen kann.

PG/PC-Applikationen wie NCM Diagnose oder STEP 7 können über eine gesicherte Tunnelverbindung auf Geräte oder Netzwerke zugreifen, die sich in einem durch das Security-Modul geschützten internen Netz befinden.



Automatische Kommunikation über VPN

Wichtig für Ihre Anwendung ist, dass der SOFTNET Security Client erkennt, wenn ein Zugriff auf die IP-Adresse eines VPN-Teilnehmers erfolgt. Adressieren Sie den Teilnehmer über die IP-Adresse so, als würde er sich im lokalen Subnetz befinden, an dem auch der PC/PG mit der Applikation angeschlossen ist.

ACHTUNG

Über den IPsec-Tunnel kann nur eine IP-basierte Kommunikation zwischen SSC und den Security-Modulen, sowie den internen Teilnehmern hinter den Security Modulen erfolgen. Ebene2-Kommunikation ist mit dem SSC nicht möglich.

Bedienung



Die PC-Software SOFTNET Security Client dient zur Konfiguration der Security-Eigenschaften, welche zur Kommunikation mit durch Security-Module geschützten Geräten notwendig sind. Nach der Konfiguration läuft der SOFTNET Security Client im Hintergrund ab, sichtbar durch ein Symbol in der Symbolleiste auf dem PG/PC.

Details in der Online-Hilfe



Detaillierte Informationen zu den Dialogen und Eingabefeldern finden Sie auch in der Online-Hilfe der Bedienoberfläche des SOFTNET Security Client.

Sie erreichen die Online-Hilfe über die Schaltfläche "Hilfe" oder über die F1-Taste.

Wie funktioniert der SOFTNET Security Client?

Der SOFTNET Security Client liest die vom Projektierwerkzeug Security Configuration Tool erstellte Konfiguration ein und ermittelt aus der Datei die zu importierenden Zertifikate. Das Root-Certificate und die Private Keys werden importiert und im lokalen PG/PC abgelegt.

Anschließend werden mit den Daten aus der Konfiguration Security-Einstellungen vorgenommen, damit Applikationen auf IP-Adressen auf und hinter den Security-Modulen zugreifen können.

Ist der Lernmodus für die internen Teilnehmer bzw. Automatisierungsgeräte aktiviert, stellt das Konfigurationsmodul zunächst eine Sicherheitsrichtlinie für den gesicherten Zugriff auf die Security-Module ein. Danach ermittelt der SOFTNET Security Client die IP-Adressen der jeweils internen Teilnehmer und trägt diese in spezielle Filterlisten der Sicherheitsrichtlinie ein.

Ergebnis: Applikationen wie z. B. STEP 7 kommunizieren über VPN mit den Automatisierungsgeräten.

ACHTUNG

Auf einem Windows-System sind die IP-Sicherheitsrichtlinien benutzerspezifisch hinterlegt. Unter einem Benutzer kann jeweils nur eine IP-Sicherheitsrichtlinie gültig sein.

Wenn eine vorhandene IP-Sicherheitsrichtlinie nicht durch die Installation des SOFTNET Security Client überschrieben werden soll, nehmen Sie die Installation und Nutzung des SOFTNET Security Client unter einem speziell dafür eingerichteten Benutzer vor.

Unterstützte Betriebssysteme

Der SOFTNET Security Client ist für den Einsatz unter den folgenden Betriebssystemen geeignet:

- Microsoft Windows XP 32 Bit + Service Pack 3
- Microsoft Windows 7 Professional 32/64 Bit
- Microsoft Windows 7 Professional 32/64 Bit + Service Pack 1
- Microsoft Windows 7 Ultimate 32/64 Bit
- Microsoft Windows 7 Ultimate 32/64 Bit + Service Pack 1

Verhalten bei Störungen

Bei auftretenden Störungen auf Ihrem PG/PC verhält sich SOFTNET Security Client wie folgt:

- Eingerichtete Sicherheitsrichtlinien bleiben über das Aus- und Einschalten Ihres PG/PC erhalten;
- Bei fehlerhafter Konfiguration werden Meldungen ausgegeben.

7.2 Installation und Inbetriebnahme des SOFTNET Security Client

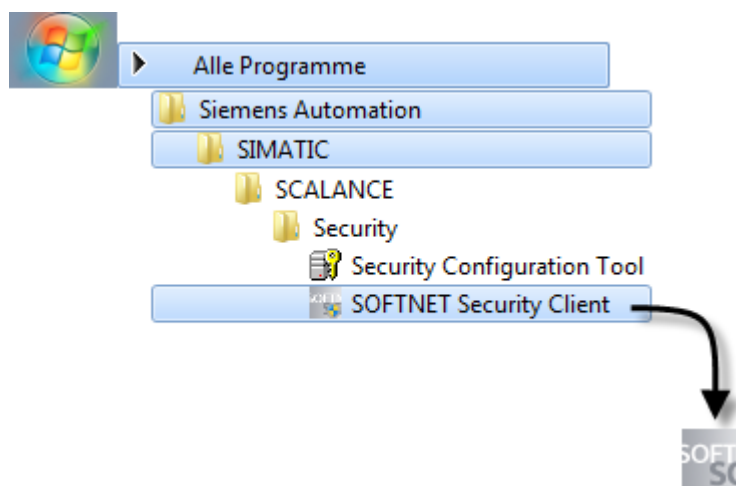
7.2.1 SOFTNET Security Client installieren und starten

Sie installieren die PC-Software SOFTNET Security Client von der Produkt CD.

1. Lesen Sie zunächst die Angaben in der LIESMICH-Datei Ihrer SCALANCE S CD und beachten Sie ggf. zusätzliche Installationshinweise.
2. Führen Sie das Setup-Programm aus;

Öffnen Sie hierzu am einfachsten die Inhaltsübersicht Ihrer SCALANCE S CD → wird beim CD-Einlegen automatisch gestartet oder kann über die Datei start.exe geöffnet werden. Wählen Sie dann direkt den Eintrag "Installation SOFTNET Security Client"

Nach der Installation und dem Start des SOFTNET Security Client erscheint das Symbol für den SOFTNET Security Client in der Windows Taskleiste:



SOFTNET Security Client einrichten

Einmal aktiviert, laufen die wichtigsten Funktionen im Hintergrund auf Ihrem PG/PC ab.

Die Projektierung des SOFTNET Security Client erfolgt folgendermaßen:

- Exportieren einer Security-Konfiguration aus dem Projektierwerkzeug Security Configuration Tool.
- Import der Security-Konfiguration in der eigenen Oberfläche, wie im nächsten Unterkapitel beschrieben.

Anlaufverhalten

Das Laden der Sicherheitsregeln kann bis zu 15 Minuten dauern. Die CPU des PG/PC wird in dieser Zeitspanne bis zu 100% ausgelastet.

SOFTNET Security Client beenden

So beenden Sie den SOFTNET Security Client:

- Klicken Sie mit der rechten Maustaste auf das SOFTNET Security Client Symbol und wählen Sie die Option "Beende SOFTNET Security Client".
- Klicken Sie in der geöffneten Oberfläche auf die Schaltfläche "Beenden".

Ergebnis: Der SOFTNET Security Client wird beendet und die Sicherheitsrichtlinie deaktiviert.

7.2.2 SOFTNET Security Client deinstallieren

Bei der Deinstallation werden die vom SOFTNET Security Client eingestellten Security-Eigenschaften zurückgesetzt.

7.3 Konfigurationsdatei mit Projektierwerkzeug Security Configuration Tool erstellen

SOFTNET Security Client-Modul im Projekt konfigurieren

Der SOFTNET Security Client wird im Projekt als Modul angelegt. Im Gegensatz zu den Security-Modulen müssen Sie keine weiteren Eigenschaften projektieren.

Weisen Sie das SSC-Modul der oder den VPN Gruppen zu, in denen IPsec-Tunnel zum PG/PC eingerichtet werden sollen. Dabei werden die Gruppeneigenschaften übernommen, die Sie für diese Gruppen projiziert haben.

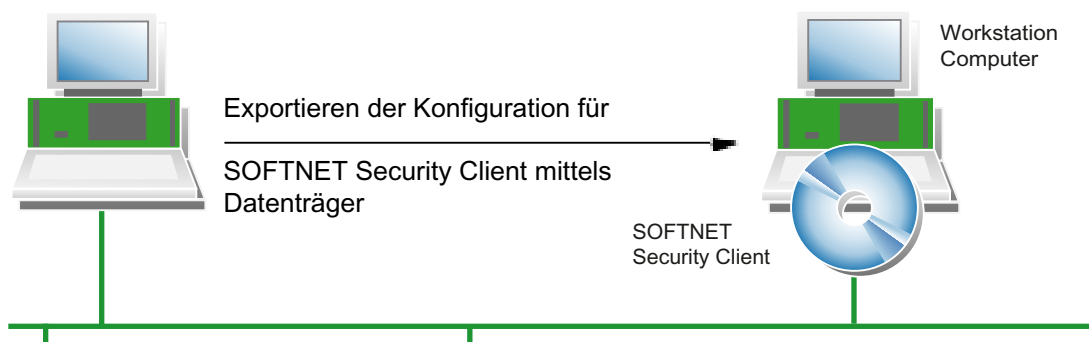
ACHTUNG
Beachten Sie die Angaben zu den Parametern im Kapitel Security-Modul in konfigurierte Gruppe aufnehmen (Seite 173).

Hinweis

Wenn Sie mehrere SOFTNET Security Clients innerhalb einer Gruppe anlegen, werden keine Tunnel zwischen diesen Clients aufgebaut, sondern nur vom jeweiligen Client zu den Security-Modulen.

Konfigurationsdateien für den SOFTNET Security Client

Die Schnittstelle zwischen dem Projektierwerkzeug Security Configuration Tool und dem SOFTNET Security Client wird über Konfigurationsdateien bedient.



Die Konfiguration wird in folgenden Dateitypen hinterlegt:

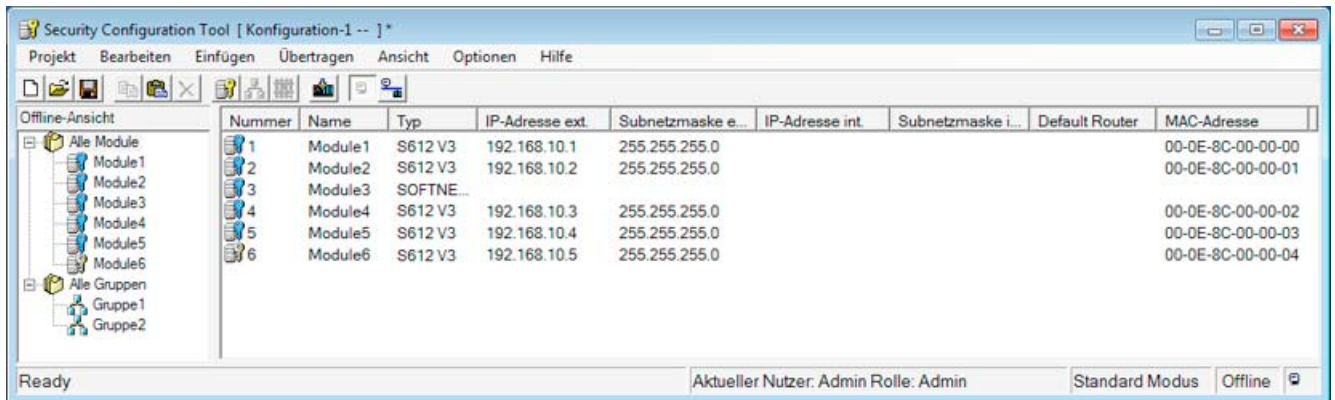
- *.dat
- *.p12
- *.cer

Vorgehensweise

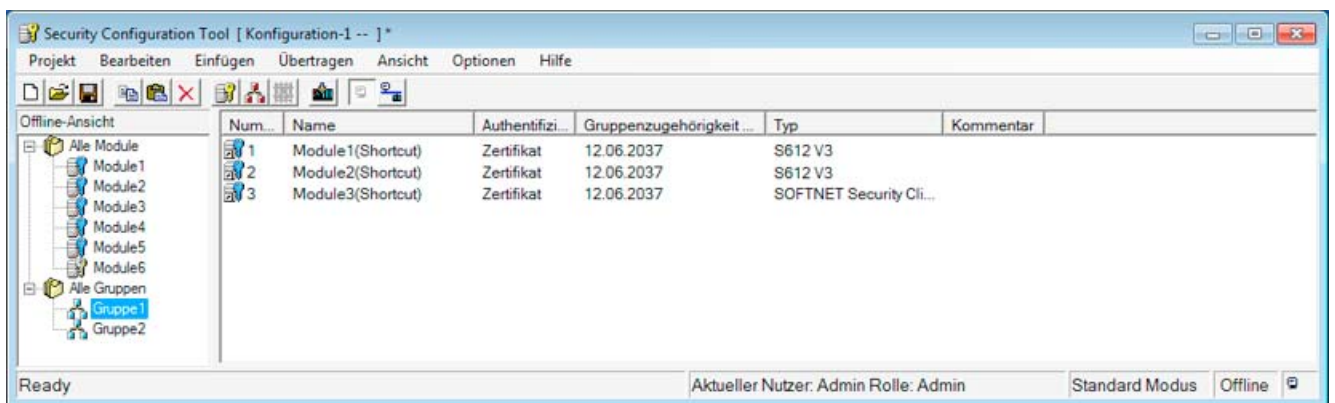
Um die Konfigurationsdateien zu erzeugen, führen Sie in SCT folgende Schritte aus:

1. Legen Sie in SCT ein Modul vom Typ SOFTNET Security Client an.

7.3 Konfigurationsdatei mit Projektierwerkzeug Security Configuration Tool erstellen



- Ordnen Sie das Modul den VPN-Gruppen zu, in denen der PG/PC über IPsec-Tunnel kommunizieren soll.



- Wählen Sie im Kontextmenü des SOFTNET Security Client den Menübefehl "Übertragen" > "An Modul...".
- Wählen Sie den Speicherort für die Konfigurationsdateien.
- Wenn Sie als Authentifizierungsmethode "Zertifikat" gewählt haben, geben Sie ein Passwort für das Zertifikat der VPN-Konfiguration an. Vergeben Sie kein Passwort, wird der Projektname (nicht das Projektpasswort) als Passwort übernommen.

Ergebnis: Der Export der Konfigurationsdateien ist abgeschlossen.

- Übernehmen Sie die Dateien vom Typ *.dat, *.p12, *.cer auf den PG/PC, auf dem Sie den SOFTNET Security Client betreiben möchten.

7.4 SOFTNET Security Client bedienen

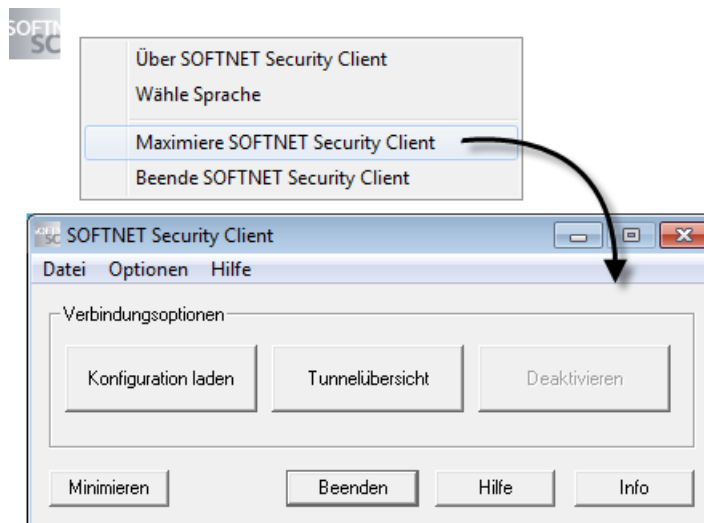
Konfigurierbare Eigenschaften

Im Einzelnen können Sie folgende Dienste nutzen:

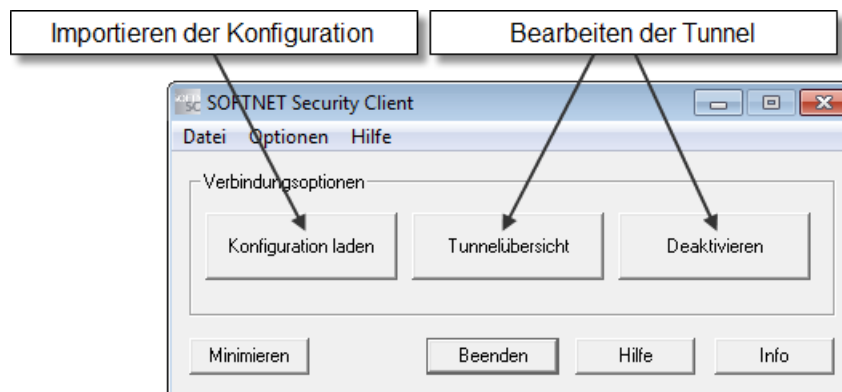
- Einrichten von sicherer IPsec-Tunnelkommunikation (VPN) zwischen dem PC/PG und allen Security-Modulen oder einzelnen Security-Modulen eines Projektes. Über diese IPsec-Tunnel kann der PC/PG auf das Security-Modul und die internen Knoten des VPN zugreifen.
- Aus- und Einschalten von bereits eingerichteten sicheren Verbindungen;
- Verbindungen bei nachträglich hinzugefügten Endgeräten einrichten. Dazu muss der Lernmodus aktiviert sein.
- Überprüfen einer Konfiguration, d. h. welche Verbindungen sind eingerichtet oder möglich.

So rufen Sie SOFTNET Security Client für die Konfiguration auf

Doppelklicken Sie auf das Symbol in der Windows Taskleiste oder wählen Sie über das Kontextmenü den Menüpunkt "Öffne SOFTNET Security Client".



Über die Schaltflächen erreichen Sie folgende Funktionen:



Schaltfläche	Bedeutung
Konfigurationsdaten laden	Dialog zur Auswahl einer Konfigurationsdatei für den Import Wählen Sie eine Datei aus und klicken auf die Schaltfläche "Öffnen". Ergebnis: Die Konfiguration wird eingelesen. Im Dialog wird abgefragt, ob die Tunnel für alle Security-Module sofort eingerichtet werden sollen. Falls in der Konfiguration IP-Adressen der Security-Module eingetragen sind oder der Lernmodus aktiv ist, werden die Tunnel für alle konfigurierten oder ermittelten Adressen eingerichtet. Diese Vorgehensweise ist besonders bei kleinen Konfigurationen schnell und effizient. Optional können Sie im Dialog für "Tunnelübersicht" alle Tunnel einrichten. Anmerkung: Sie können nacheinander die Konfigurationsdateien aus mehreren im SCT erstellten Projekten importieren (siehe auch nachfolgende Erläuterung zur Vorgehensweise).
Tunnelübersicht	Dialog zum Einrichten und Bearbeiten der Tunnel Über diesen Dialog nehmen Sie die eigentliche Konfiguration des SOFTNET Security Client vor. Es wird eine Liste der gesicherten Tunnel mit den IP-Adressen der Security-Module angezeigt. Falls auf Ihrem PG/PC mehrere Netzwerkkadaper vorhanden sind, wählt der SOFTNET Security Client automatisch einen aus über den ein Tunnelaufbau versucht wird. Gegebenenfalls konnte der SOFTNET Security Client jedoch keinen zu ihrem Teilnehmer passenden finden und hat einen beliebigen eingetragen. In diesem Fall müssen Sie die Netzwerkkadapereinstellung über den Dialog "Netzwerkkadaper" im Kontextmenü der Teilnehmer und Security-Module manuell anpassen
Deaktivieren	Alle gesicherten Tunnel deaktivieren
Minimieren	Die Bedienoberfläche des SOFTNET Security Client wird geschlossen Das Symbol für den SOFTNET Security Client wird weiterhin in der Windows Taskleiste angezeigt.
Beenden	Der SOFTNET Security Client wird beendet und alle Tunnel deaktiviert.
Hilfe	Online-Hilfe aufrufen
Info	Informationen zum Ausgabestand des SOFTNET Security Client Details: Liste aller für die Funktion des SOFTNET Security Client benötigten Dateien mit Rückmeldung, ob diese auf dem System gefunden werden konnten

7.5 Tunnel einrichten und bearbeiten

Einrichten von sicheren Verbindungen zu allen Security-Modulen

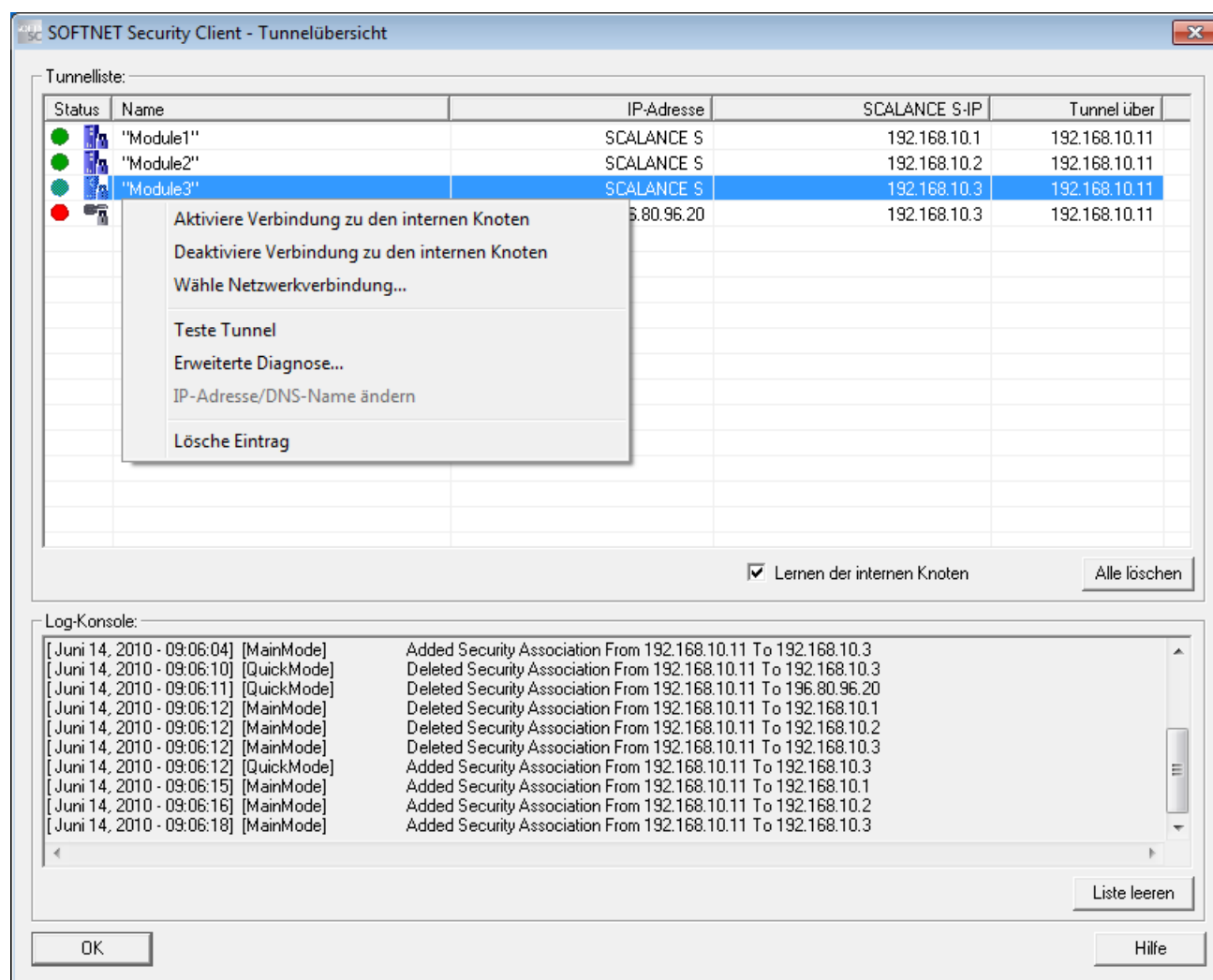
Im Dialog für den Konfigurationsimport wählen Sie, ob die Tunnel für alle Security-Module sofort eingerichtet werden sollen. Dadurch ergeben sich die folgenden Möglichkeiten:

- Tunnel automatisch aktivieren

Falls in der Konfiguration die IP-Adressen der Security-Module eingetragen sind oder der Lernmodus aktiv ist, werden die Tunnel für alle konfigurierten oder ermittelten Adressen eingerichtet.

- Tunnelkonfiguration nur einlesen

Optional können Sie die konfigurierten Tunnel nur einlesen und anschließend im Dialog für das Einrichten der Tunnel einzeln aktivieren.



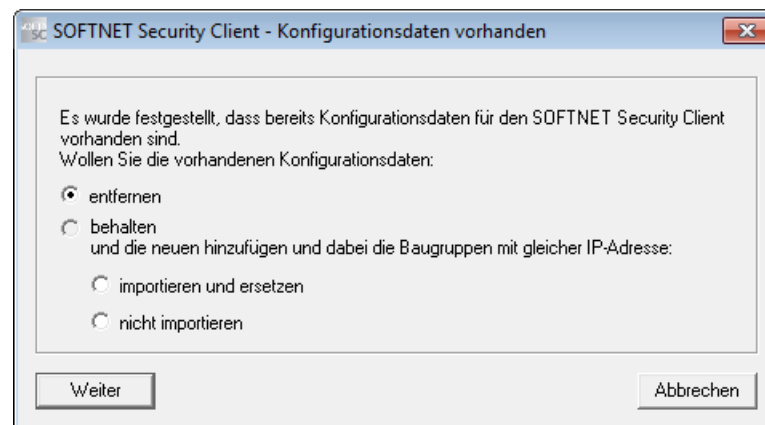
So richten Sie die Tunnelverbindungen ein

1. Öffnen Sie den Dialog zum Import der Konfigurationsdatei über die Schaltfläche "Konfigurationsdaten einlesen".

2. Wählen Sie die mit SCT erstellte Konfigurationsdatei aus.

Sie können Konfigurationsdaten aus mehreren Projekten gleichzeitig einlesen. Falls im SOFTNET Security Client bereits Konfigurationsdaten vorliegen, wählen Sie eine der folgenden Optionen aus:

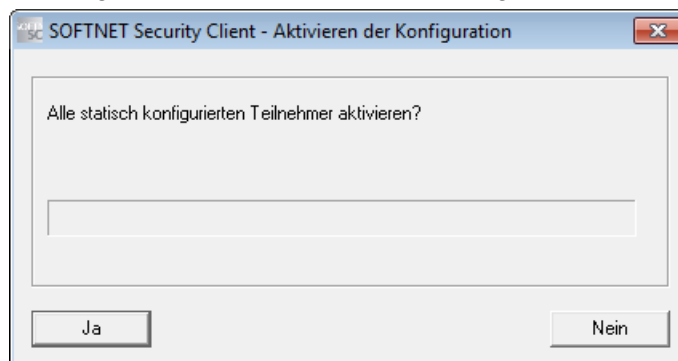
- "entfernen": Nur die zuletzt geladenen Konfigurationsdaten sind verfügbar.
- "importieren und ersetzen": Ist bei geänderten Konfigurationsdaten sinnvoll, beispielsweise nur die Konfiguration im Projekt a ist geändert, Projekt b und c bleiben erhalten.
- "nicht importieren": ist sinnvoll, wenn in einem Projekt ein Security-Modul hinzugefügt wurde, ohne dass bereits gelernte interne Knoten verloren gehen.



3. Wenn Sie in SCT als Authentifizierungsmethode "Zertifikat" gewählt haben, geben Sie das Passwort ein.

4. Wählen Sie aus, ob für die in der Konfiguration projektierten Teilnehmer (statisch konfigurierte Teilnehmer) die Tunnelverbindungen aktiviert werden sollen.

Falls Sie die Aktivierung hier noch nicht anstoßen, können Sie dies jederzeit im nachfolgend beschriebenen Tunnel-Dialog durchführen.

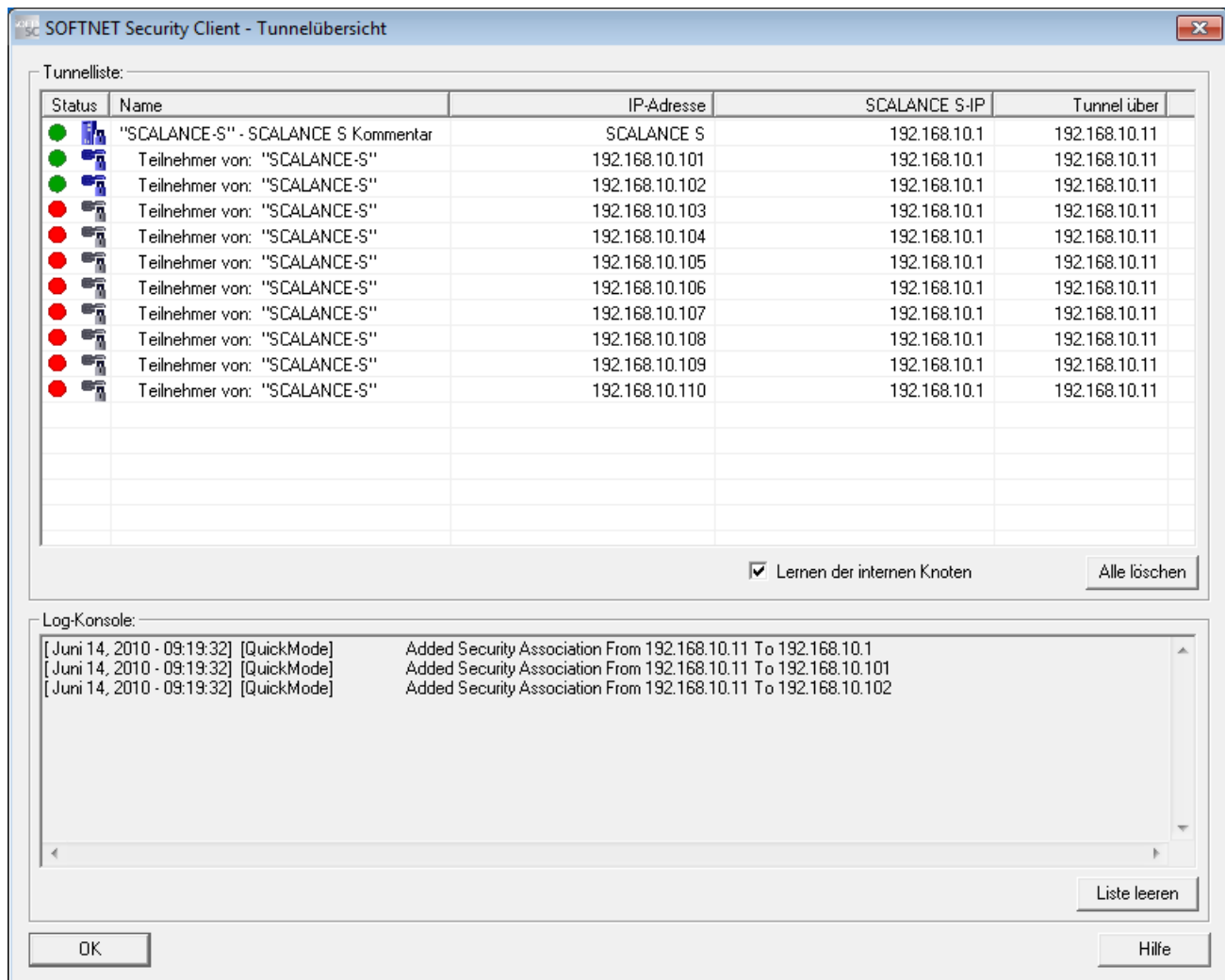


Wenn Sie die Aktivierung der Tunnelverbindungen gewählt haben, werden nun die Tunnelverbindungen zwischen dem SOFTNET Security Client und den Security-Modulen aufgebaut.

Dies kann mehrere Sekunden dauern.

5. Öffnen Sie den Dialog "Tunnelübersicht".

In der Tabelle werden die Module und Teilnehmer mit Statusinformationen zu den Tunnelverbindungen angezeigt.



6. Falls Knoten bzw. Teilnehmer in der Tabelle nicht angezeigt werden, setzen Sie über die Kommandozeile ein Ping-Kommando an den fehlenden Knoten ab.

Ergebnis: Der Knoten wird vom Security-Modul gelernt und an den SOFTNET Security Client weitergegeben.

Anmerkung:

Falls der Dialog nicht geöffnet ist während ein Teilnehmer erfasst wird, wird der Dialog automatisch aufgeblendet.

Hinweis

Statisch konfigurierte Teilnehmer und Subnetze

Wenn Sie Teilnehmer oder Subnetze statisch konfigurieren, müssen Sie auch die Konfiguration für einen in der VPN-Gruppe genutzten SOFTNET Security Client neu laden.

7. Aktivieren Sie die Teilnehmer, bei denen noch keine Tunnelverbindung aufgebaut ist.
- Nach erfolgreichem Verbindungsaufbau starten Sie die Applikation, die eine Kommunikationsverbindung zu einem der Teilnehmer aufbauen soll, z. B. STEP 7.

ACHTUNG

Wenn auf dem PG/PC mehrere Netzwerkadapter vorhanden sind, wählt SSC den Netzwerkadapter zum Aufbau eines Tunnels automatisch aus. Falls kein zum Projekt passender Netzwerkadapter vorhanden ist, trägt SSC automatisch einen ein. Passen Sie in diesem Fall die Einstellung zum Netzwerkadapter über das Kontextmenü der Teilnehmer und Security-Module an.

Bedeutung der Parameter

Tabelle 7- 1 Parameter im Dialogfeld "Tunnelübersicht"

Parameter	Bedeutung / Wertebereich
Status	Mögliche Statusanzeigen finden Sie in der nachfolgenden Tabelle.
Name	Aus der SCT-Konfiguration übernommener Name des Moduls oder des Teilnehmers.
Int. Teilnehmer-IP / Subnetz	Wenn interne Teilnehmer / Subnetze vorhanden sind, wird die IP-Adresse des internen Knotens bzw. die Netz-ID des internen Subnetzes angezeigt.
Tunnelendpunkt-IP	IP-Adresse des zugeordneten Security-Moduls.
Tunnel über...	Falls der PC mit mehreren Netzwerkkarten betrieben wird, wird die zugeordnete IP-Adresse angezeigt, über welche der VPN-Tunnel aufgebaut wird.

Tabelle 7- 2 Statusanzeigen

Symbol	Bedeutung
	Es besteht keine Verbindung zum Modul oder Teilnehmer.
	Es sind weitere Teilnehmer vorhanden, die nicht angezeigt werden. Doppelklicken Sie auf das Symbol, um weitere Teilnehmer anzuzeigen.
	Der Teilnehmer ist nicht aktiviert.
	Der Teilnehmer ist aktiviert.
	Deaktiviertes Security-Modul.
	Aktiviertes Security-Modul..

Symbol	Bedeutung
	Deaktiviertes SCALANCE M-Modul.
	Aktiviertes SCALANCE M-Modul.
	Internes Subnetz deaktiviert.
	Internes Subnetz aktiviert.
	Modul / Teilnehmer ist nicht erreichbar.
	Modul / Teilnehmer ist erreichbar.
	Erreichbarkeitstest deaktiviert.

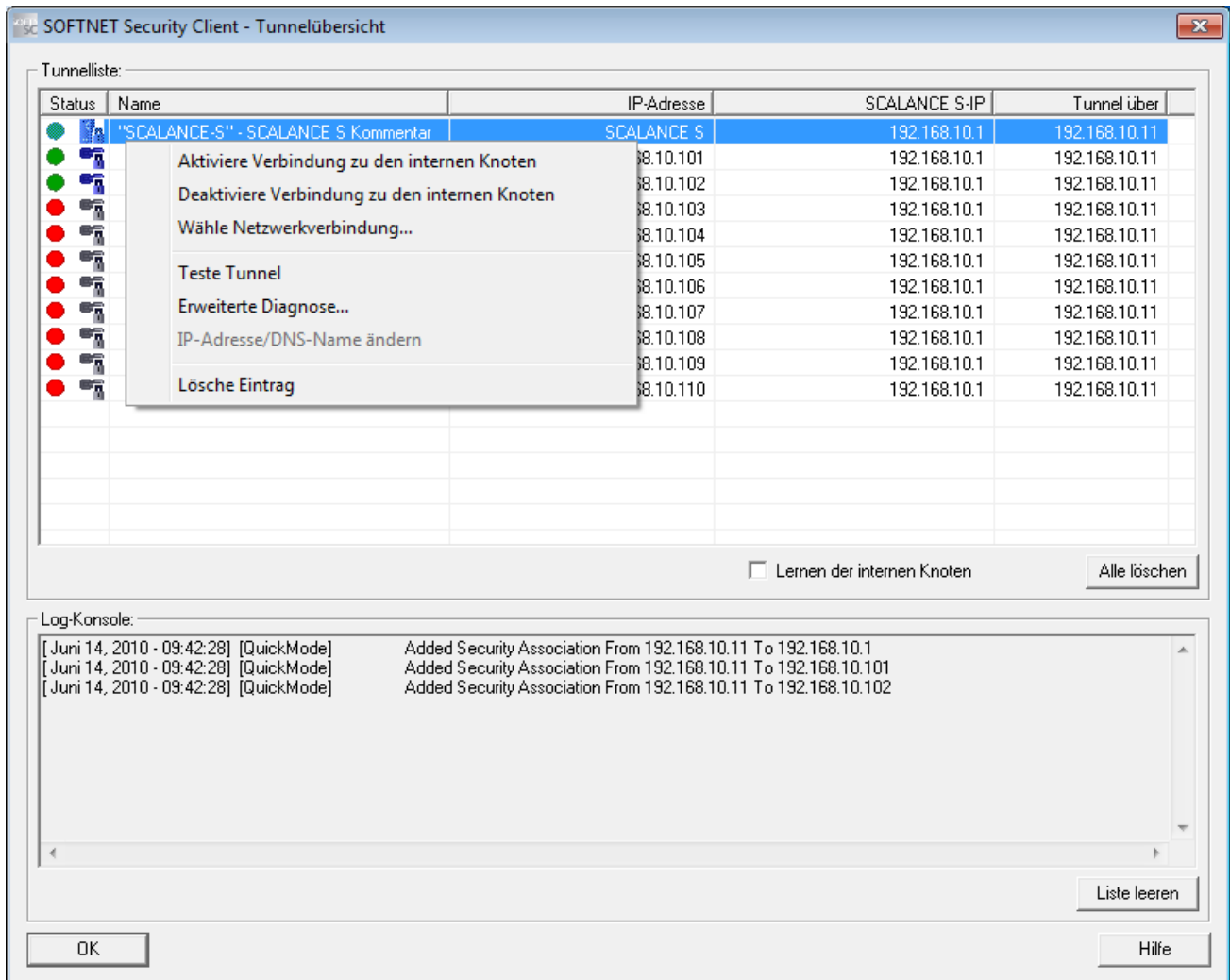
Optionskästchen "Lernen der internen Knoten"

Ist in der Konfiguration der Security-Module der Lernmodus aktiviert, kann dieser auch für den SOFTNET Security Client aktiviert werden. Dadurch erhalten Sie automatisch die Informationen über die internen Teilnehmer der Security-Module.

Ansonsten ist das Auswahlfeld "Lernen der internen Knoten" inaktiv.

Tunnel-Eintrag selektieren und bedienen

Wählen Sie im Dialog "Tunnelübersicht" einen Eintrag aus und öffnen Sie über das Kontextmenü weitere Optionen.



ACHTUNG

Wenn für einen Netzwerkadapter mehrere IP-Adressen verwendet werden, weisen Sie im Dialog "Tunnelübersicht" jedem Eintrag die IP-Adresse zu.

Schaltfläche "Alle löschen"

Die IP-Sicherheitsrichtlinie und alle nicht über SSC eingerichteten Einträge werden gelöscht.

Aus- und Einschalten von bereits eingerichteten sicheren Verbindungen

Eingerichtete sichere Verbindungen schalten Sie über die Schaltfläche "Deaktivieren" aus. Nach Klicken der Schaltfläche ändert sich der Text in der Schaltfläche auf "Aktivieren" und das Symbol in der Statusleiste wird ersetzt.

Ergebnis: Auf dem PC ist die Security Policy deaktiviert.

Um die Änderung rückgängig zu machen und die eingerichteten Tunnel wieder zu aktivieren, klicken Sie auf die Schaltfläche "Aktivieren".

Log-Konsole

Welche Einträge in der Log-Konsole angezeigt werden, wählen Sie im Dialog "Einstellungen" aus.

- Diagnoseinformationen zum Verbindungsaufbau mit den konfigurierten Security-Modulen / SCALANCE M-Modulen und internen Teilnehmern / Subnetzen.
- Datums- und Zeitstempel zum Zeitpunkt der Ereignisse
- Auf- und Abbau einer Security Association
- Negativ verlaufener Erreichbarkeitstest (Test-Ping) zu den konfigurierten Teilnehmern

Schaltfläche "Liste leeren"

Löscht alle Einträge in der Log-Konsole.

Globale Einstellungen für den SOFTNET Security Client

1. Öffnen Sie im Hauptdialog des SOFTNET Security Client den Menüpunkt "Optionen" > "Einstellungen".
2. Nehmen Sie globale Einstellungen vor, die nach dem Beenden und Öffnen des SOFTNET Security Client erhalten bleiben.

Die Funktionen entnehmen Sie aus der folgenden Tabelle.

Funktion	Beschreibung / Optionen
Log-File Größe (Log-Konsole)	Log-File Größe der Quelldatei, welche die Meldungen enthält, die gefiltert und auf eine bestimmte Anzahl begrenzt in der Log-Konsole der Tunnelübersicht ausgegeben werden.
Anzahl anzuzeigender Meldungen in Log-Konsole der Tunnelübersicht	Anzahl der Meldungen, welche aus dem Log-File der Quelldatei extrahiert und in der Log-Konsole der Tunnelübersicht angezeigt werden.

Funktion	Beschreibung / Optionen
Folgende Log-Meldungen in Log-Konsole der Tunnelübersicht ausgeben: • Anzeige des negativen Erreichbarkeitstest (Ping) • Anlegen / Löschen von Security Associations (Quick Modes) • Anlegen / Löschen von Main Modes • Laden von Konfigurationsdateien • Lernen interner Teilnehmer	Meldungen, welche in der Log-Konsole der Tunnelübersicht optional angezeigt werden.
Logfile-Größe (Debug-Logfiles)	Logfile-Größe der Quelldateien für Debug-Meldungen des SOFTNET Security Client (können vom Customer Support angefordert werden, um Analysen zu erleichtern)
Erreichbarkeitstest, Wartezeit auf Rückantwort	Einstellbare Wartezeit für den Ping, welcher die Erreichbarkeit eines Tunnelpartners angeben soll. Vor allem einzustellen bei Tunneln mit langsamen Übertragungswegen (UMTS, GPRS, etc.), bei denen die Laufzeit der Datenpakete deutlich höher ist. Beeinflusst somit direkt die Anzeige der Erreichbarkeit in der Tunnelübersicht.
Erreichbarkeitstest global deaktivieren	Wenn Sie diese Funktion aktivieren, wird der Erreichbarkeitstest global für alle enthaltenen Konfigurationen im SOFTNET Security Client deaktiviert. Vorteil: Keine zusätzlichen Pakete erzeugen Datenvolumen Nachteil: Sie erhalten in der Tunnelübersicht keine Rückmeldung, ob ein Tunnelpartner erreichbar ist oder nicht.

Erweiterte Moduldiagnose

Öffnen Sie im Hauptdialog des SOFTNET Security Client den Menüpunkt "Optionen" > "Erweiterte Moduldiagnose".

Die Ansicht dient nur der Diagnose des Systemzustandes im Zusammenhang mit den konfigurierten Security-Modulen und kann bei Anfragen beim Customer Support helfen.

- Security-Modul

Wählen Sie das Modul aus, für das der aktuelle Systemstatus diagnostiziert werden soll.

- RoutingEinstellungen (Modulspezifische Parameter)

Zeigt die aus der Konfiguration ermittelten Einstellungen zu Schnittstellen und internen Knoten/Subnetzen an.

- **Aktive Main Modes / Aktive Quick Modes**

Sind für das ausgewählte Modul auf dem PG/PC Main Modes bzw. Quick Modes eingerichtet, werden die dazugehörigen Details hier angezeigt. Dazu gehört auch die gesamte Anzahl der Main Modes bzw. Quick Modes, die zu dem ausgewählten Modul auf dem System gefunden wurden.

- **RoutingEinstellungen (Netzwerkeinstellungen des Rechners)**

Zeigt die aktuellen Routing-Einstellungen des Rechners an.

Über die Option "Alle RoutingEinstellungen anzeigen" erhalten Sie zusätzliche Routing-Angaben.

- **Zugewiesene IP-Adressen**

Liste über die dem Rechner bekannten Netzwerkschnittstellen in Verbindung mit den konfigurierten bzw. zugewiesenen IP-Adressen.

Online Funktionen - Test, Diagnose und Logging

Zu Test- und Überwachungszwecken verfügt das Security-Modul über Diagnose- und Logging-Funktionen.

- **Diagnosefunktionen**

Hierunter sind verschiedene System- und Statusfunktionen zu verstehen, die Sie im Online-Modus anwenden können.

- **Logging-Funktionen**

Hierbei geht es um die Aufzeichnung von System- und Sicherheitsereignissen.

Die Aufzeichnung der Ereignisse erfolgt in Pufferbereiche des Security-Moduls oder eines Servers. Die Parametrierung und Auswertung dieser Funktionen setzt eine Netzwerkverbindung auf das ausgewählte Security-Modul voraus.

Ereignisse mit Logging-Funktionen aufzeichnen

Welche Ereignisse aufgezeichnet werden sollen, legen Sie mit den Log-Einstellungen zum jeweiligen Security-Modul fest.

Dabei können Sie für die Aufzeichnung folgende Varianten konfigurieren:

- **Lokales Logging**

Bei dieser Variante zeichnen Sie die Ereignisse in lokalen Puffern des Security-Moduls auf. Im Online-Dialog des Security Configuration Tool können Sie dann auf diese Aufzeichnungen zugreifen, diese sichtbar machen und in der Service-Station archivieren.

- **Netzwerk Syslog**

Beim Netzwerk Syslog nutzen Sie einen im Netz vorhandenen Syslog-Server. Dieser zeichnet die Ereignisse entsprechend der Konfiguration in den Log-Einstellungen des jeweiligen Security-Moduls auf.

Log-Daten archivieren und aus Datei einlesen

Sie können die aufgezeichneten Ereignisse zur Archivierung in einer Log-Datei speichern und diese auch im Offline-Modus öffnen. Weitere Informationen finden Sie im Kapitel Funktionsübersicht Online-Dialog (Seite 204).

8.1 Funktionsübersicht Online-Dialog

Das Security-Modul bietet im Security Configuration Tool folgende Funktionen im Online-Dialog:

Tabelle 8- 1 Funktionen und Logging in der Online-Diagnose

Funktion / Register im Online-Dialog		Bedeutung
System- und Statusfunktionen		
	Zustand	Anzeige des Geräte-Status des im Projekt angewählten Security-Moduls.
	Datum und Uhrzeit	Einstellung von Datum und Uhrzeit.
	Schnittstellen-Einstellungen	Übersicht zu den Einstellungen der einzelnen Schnittstellen.
	Cache-Tabellen	Anzeige der ARP-Tabelle des Security-Moduls.
	Benutzer-Kontrolle	Anzeige der Benutzer, die an der Internetseite für benutzerspezifische IP-Regelsätze angemeldet sind.
	Kommunikationszustand	Anzeige des Kommunikations-Status und der internen Netzknoten zu weiteren der VPN-Gruppe zugehörigen Security-Modulen.
 	Interne Knoten	Anzeige der internen Netzknoten des Security-Moduls.
	Dynamisch aktualisierte Firewall-Regeln	Anzeige der IP-Adressen, die bei der Verwendung von IP Access Control-Listen dynamisch über FTP oder HTTP freigeschaltet oder von einem Benutzer nachgeladen wurden.
Logging-Funktionen		
	System-Log	Anzeige von geloggten System-Ereignissen.
	Audit-Log	Anzeige von geloggten Sicherheits-Ereignissen.
	Paketfilter-Log	Anzeige von geloggten Daten-Paketen, sowie Starten und Stoppen des Paket-Logging.



Nähere Informationen zu den Einstellmöglichkeiten in den einzelnen Registern erhalten Sie in der Online-Hilfe.

Zugriffsvoraussetzungen

Damit Sie an einem Security-Modul die Online-Funktionen nutzen können, müssen folgende Voraussetzungen erfüllt sein:

- eine Netzwerkverbindung zum ausgewählten Modul besteht
- das Projekt, mit dem das Modul konfiguriert wurde, ist geöffnet
- die Online-Betriebsart im Security Configuration Tool ist eingeschaltet

Hinweis

Auswirkung der Betriebsart vom Security Configuration Tool

Sie können Diagnosefunktionen, die nur im Erweiterten Modus zur Verfügung stehen, auch dann verwenden, wenn Sie das Projekt im Standard Modus erstellt haben.

So erreichen Sie diese Funktion

1. Wechseln Sie über den Menübefehl "Ansicht" > "Online" die Betriebsart.
2. Markieren Sie das zu bearbeitende Modul.
3. Wählen Sie den Menübefehl "Bearbeiten" > "Online Diagnose...".

Sobald Sie eines der Register für Log-Funktionen öffnen, sehen Sie im unteren Bereich des Registers den aktuellen Zustand der Aufzeichnungsfunktion des gewählten Security-Moduls:

- Puffer-Einstellungen: Umlaufspeicher / Linearer Speicher

Der aktuelle Aufzeichnungszustand kommt aus der geladenen Konfiguration oder aus der zuvor schon einmal durchgeführten Online-Funktion.

Warnmeldung bei nicht aktueller Konfiguration oder Fremdprojekt

Wenn Sie den Online-Dialog aufrufen, wird geprüft, ob die aktuelle Konfiguration auf dem Security-Modul und die Konfiguration des geladenen Projekts übereinstimmen.

Unterscheiden sich die beiden Konfigurationen, so wird eine Warnmeldung ausgegeben.

Dadurch wird signalisiert, dass Sie entweder die Konfiguration (noch) nicht aktualisiert haben, oder das falsche Projekt verwenden.

Online-Einstellungen werden nicht in der Konfiguration gespeichert

Einstellungen, die Sie in der Online-Betriebsart vornehmen (z. B. Einstellungen zum Log-Speicher), werden nicht in der Konfiguration auf dem Security-Modul gespeichert. Nach einem Modul-Neuanlauf sind deshalb immer die Einstellungen aus der Konfiguration wirksam.

8.2 Ereignisse aufzeichnen (Logging)

Übersicht

Ereignisse auf dem Security-Modul können aufgezeichnet werden. Die Aufzeichnung erfolgt je nach Ereignistyp in flüchtige oder dauerhafte lokale Pufferbereiche. Alternativ kann auch eine Aufzeichnung in einem Netzwerk-Server erfolgen.

Konfiguration im Standard Modus und im Erweiterten Modus

Die Auswahlmöglichkeiten im Security Configuration Tool hängen von der gewählten Ansicht ab:

- Standard Modus

"Lokales Logging" ist im Standard Modus standardmäßig aktiviert; Paketfilter-Ereignisse können global im Register "Firewall" aktiviert werden. "Netzwerk Syslog" ist in dieser Ansicht nicht möglich.

- Erweiterter Modus

Sämtliche Logging-Funktionen können aktiviert oder deaktiviert werden; Paketfilter-Ereignisse müssen selektiv im Register "Firewall" (lokale oder globale Regeln) aktiviert werden.

Aufzeichnungsverfahren und Ereignisklassen

Sie können in der Konfiguration festlegen, welche Daten aufgezeichnet werden sollen. Dadurch aktivieren Sie die Aufzeichnung bereits mit dem Laden der Konfiguration in das Security-Modul.

Außerdem wählen Sie in der Konfiguration eine oder beide der möglichen Aufzeichnungsverfahren:

- Lokales Logging
- Netzwerk Syslog

Das Security-Modul kennt für beide Aufzeichnungsverfahren die folgenden Ereignisse:

Funktion / Register im Online-Dialog	Funktionsweise
Paketfilter-Ereignisse (Firewall)	Der Paketfilter-Log zeichnet bestimmte Pakete des Datenverkehrs auf. Es werden nur Datenpakete geloggt, auf die eine projektierte Paketfilter-Regel (Firewall) zutrifft, oder auf die der Basisschutz reagiert (korrupte bzw. ungültige Pakete). Voraussetzung ist, dass die Aufzeichnung für die Paketfilter-Regel aktiviert ist.
Audit-Ereignisse	Der Audit-Log zeichnet automatisch fortlaufend sicherheitsrelevante Ereignisse auf, wie z. B. Benutzeraktionen wie das Ein- oder Ausschalten des Paket-Logging oder Aktionen, bei denen sich ein Benutzer nicht korrekt über Passwort authentisiert hat.
System-Ereignisse	Das System-Log zeichnet automatisch fortlaufend Systemereignisse wie z. B. den Start eines Prozesses auf. Anhand von Ereignisklassen ist die Aufzeichnung skalierbar.
	Leitungsdiagnose: Zusätzlich ist eine Leitungsdiagnose projektierbar. Die Leitungsdiagnose liefert Meldungen, sobald die Anzahl fehlerhafter Telegrammpakete einen einstellbaren Grenzwert überschritten hat. 

Speicherverfahren für die Datenaufzeichnung beim lokalen Logging

Die Speicherung bei der Datenaufzeichnung erfolgt nach zwei wählbaren Verfahren:

- Umlaufspeicher

Bei Erreichen des Pufferendes wird die Aufzeichnung am Pufferanfang mit dem Überschreiben der ältesten Einträge fortgesetzt.

- Linearer Speicher

Die Aufzeichnung stoppt, wenn der Puffer voll ist.

Ein- bzw. Ausschalten des Logging

In der Betriebsart "Offline" können Sie über die Log-Einstellungen das lokale Logging für die Ereignisklassen aktivieren und das Speicherverfahren festlegen. Diese Log-Einstellungen werden mit der Konfiguration in das Modul geladen und werden mit dem Start des Security-Moduls wirksam.

Sie können das lokale Logging für Paketfilter-Ereignisse und System-Ereignisse in den Online-Funktionen bei Bedarf ebenfalls aktivieren oder deaktivieren. Die Einstellungen in der Projektkonfiguration werden dadurch nicht verändert.

8.2.1 Lokales Logging - Einstellungen in der Konfiguration

In der Betriebsart "Offline" können Sie über die Log-Einstellungen die Ereignisklassen aktivieren und das Speicherverfahren festlegen. Diese Log-Einstellungen werden mit der Konfiguration in das Modul geladen und werden mit dem Start des Security-Moduls wirksam.

Sie können diese projektierten Log-Einstellungen in den Online-Funktionen bei Bedarf ändern. Die Einstellungen in der Projektkonfiguration werden dadurch nicht verändert.

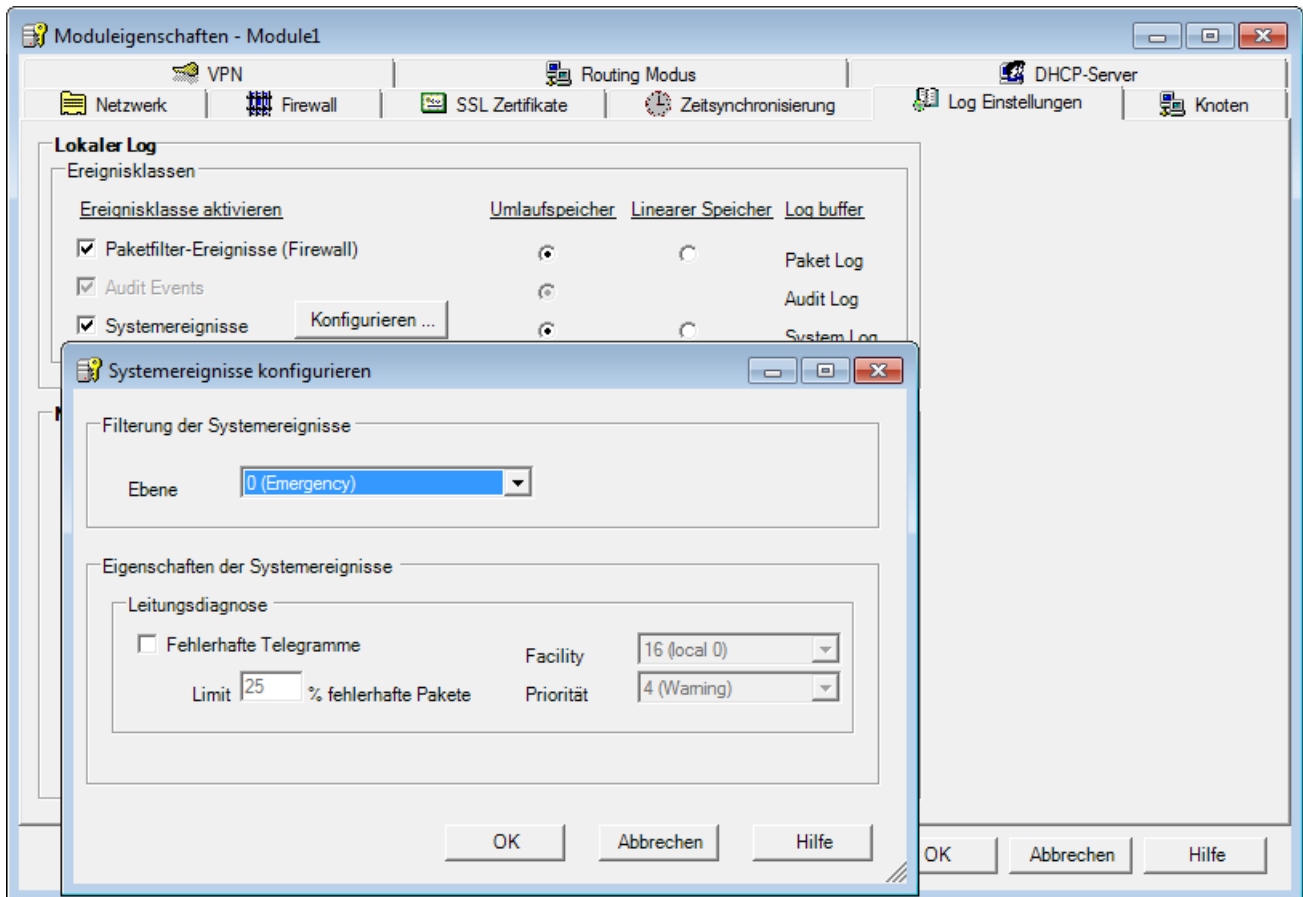
Log-Einstellungen im Standard Modus

Die Log-Einstellungen im Standard Modus entsprechen den Voreinstellungen im Erweiterten Modus. Im Standard Modus können Sie die Einstellungen jedoch nicht verändern.

Log-Einstellungen im Erweiterten Modus

1. Markieren Sie das zu bearbeitende Modul.
2. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Log-Einstellungen".

Der folgende Dialog zeigt die Standard-Einstellungen für das Security-Modul; zusätzlich ist der Dialog zur Konfiguration der Aufzeichnung von System-Ereignissen geöffnet:



Ereignisklassen konfigurieren

Tabelle 8- 2 Lokaler Log - Funktionsübersicht

Funktion / Register im Online-Dialog	Projektierung	Bemerkungen
Paketfilter-Ereignisse (Firewall)	Die Aktivierung erfolgt über Optionskästchen. Die Auswahl des Speicherverfahrens erfolgt über Optionsfelder.	Paketfilter-Logdaten sind nicht remanent Die Daten werden in einem flüchtigen Speicher des Security-Moduls abgelegt und stehen deshalb nach einem Ausschalten der Spannungsversorgung nicht mehr zur Verfügung.
Audit-Ereignisse (immer aktiviert)	Logging ist immer aktiviert. Die Speicherung erfolgt immer im Umlaufpuffer.	Audit-Logdaten sind remanent Die Daten werden in einem remanenten Speicher des Security-Moduls abgelegt und stehen deshalb auch nach einem Ausschalten der Spannungsversorgung noch zur Verfügung.

Funktion / Register im Online-Dialog	Projektierung	Bemerkungen
System-Ereignisse	Die Aktivierung erfolgt über Optionskästchen. Die Auswahl des Speicherverfahrens erfolgt über Optionsfelder. Zur Konfiguration des Ereignisfilters und der Leitungsdiagnose öffnen Sie über die Schaltfläche "Konfigurieren..." einen weiteren Dialog.	System-Logdaten sind nicht remanent Die Daten werden in einem flüchtigen Speicher des Security-Moduls abgelegt und stehen deshalb nach einem Ausschalten der Spannungsversorgung nicht mehr zur Verfügung.
Filterung der System-Ereignisse	Stellen Sie in diesem Sub-Dialog für die System-Ereignisse eine Filterebene ein. Standardmäßig sind die folgenden Werte eingestellt: • SCALANCE S: Ebene 0 • CP: Ebene 3	Wählen Sie als Filterebene "Error" oder einen höheren Wert, um die Aufzeichnung von allgemeinen, nicht kritischen Ereignissen abzustellen. Hinweis für CP Wählen Sie für den CP nur Ebene 3 oder Ebene 6 aus. • Bei Auswahl von Ebene 3 werden die Fehlermeldungen der Ebenen 0 bis 3 ausgegeben. • Bei Auswahl von Ebene 6 werden die Fehlermeldungen der Ebenen 0 bis 6 ausgegeben.
Leitungsdiagnose 	Die Leitungsdiagnose erzeugt ein spezielles System-Ereignis. Stellen Sie ein, ab welchem Prozentsatz fehlerhafter Telegramme ein System-Ereignis erzeugt werden soll. Weisen Sie dem System-Ereignis eine Facility und eine Severity zu.	Über die Severity gewichten Sie die System-Ereignisse der Leitungsdiagnose im Verhältnis zur Severity der übrigen System-Ereignisse. Hinweis Weisen Sie den System-Ereignissen der Leitungsdiagnose keine geringere Severity als der Filterung der System-Ereignisse zu. Ansonsten passieren diese Ereignisse den Filter nicht und werden nicht aufgezeichnet.

8.2.2 Netzwerk Syslog - Einstellungen in der Konfiguration

Sie können das Security-Modul als Client konfigurieren, der Logging-Informationen an einen Syslog-Server sendet. Der Syslog-Server kann sich im lokalen internen oder im externen Subnetz befinden. Die Implementierung entspricht RFC 3164.

Hinweis

Firewall - Syslog-Server im externen Netz nicht aktiv

Wenn der Syslog-Server auf dem adressierten Rechner nicht aktiv ist, sendet dieser Rechner in der Regel ICMP-Antworttelegramme "port not reachable" zurück. Wenn aufgrund der Firewall-Konfiguration diese Antworttelegramme als Systemereignisse aufgezeichnet und an den Syslog-Server gesendet werden, kann sich dieser Vorgang endlos fortsetzen (Ereignis-Lawine).

Abhilfen:

- Syslog-Server starten;
 - Firewall-Regeln ändern;
 - Rechner mit deaktiviertem Syslog-Server vom Netz nehmen;
-

Log-Einstellungen vornehmen

1. Schalten Sie über den Menübefehl "Ansicht" > "Erweiterter Modus" die Betriebsart um.

Hinweis

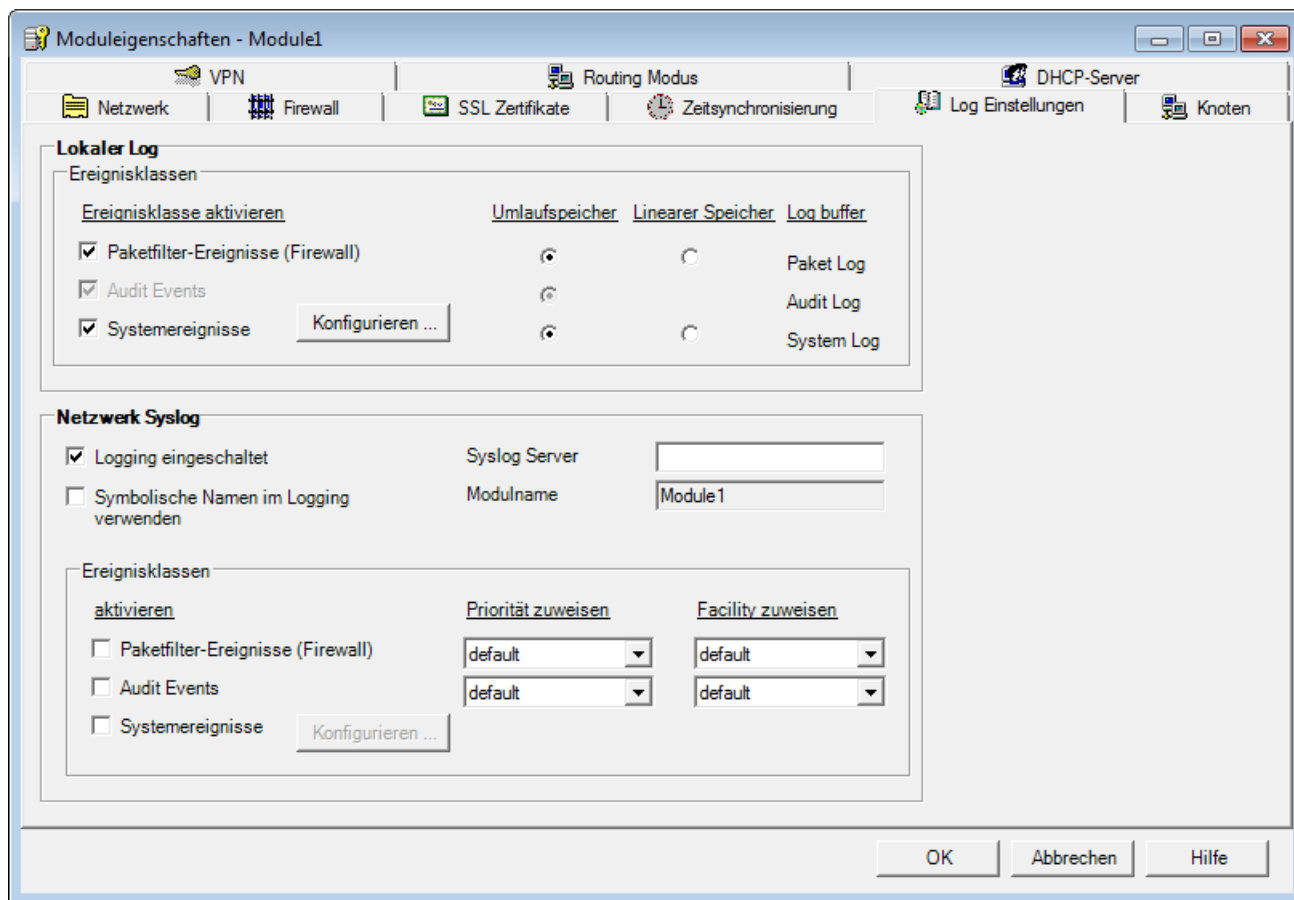
Keine Umschaltung zurück in den Standard Modus möglich

Sobald Sie die Konfiguration für das aktuelle Projekt geändert haben, können Sie eine einmal vorgenommene Umschaltung in den Erweiterten Modus nicht mehr rückgängig machen.

Abhilfe SCT Standalone: Sie schließen das Projekt ohne zu speichern und öffnen es erneut.

2. Markieren Sie das zu bearbeitende Modul.
3. Wählen Sie den Menübefehl "Bearbeiten" > "Eigenschaften...", Register "Log-Einstellungen".

Der folgende Dialog zeigt die Standard-Einstellungen für das Security-Modul bei aktiviertem Logging für das Netzwerk Syslog:



Verbindung zum Syslog-Server herstellen

Für SCALANCE S: Das Security-Modul verwendet den projektierten Modulnamen als Hostnamen gegenüber dem Syslog-Server.

Für CPs: Das Security-Modul verwendet die eigene IP-Adresse als Hostnamen gegenüber dem Syslog-Server.

Geben Sie im Feld "Syslog-Server" die IP-Adresse des Syslog-Servers ein. Sie können die IP-Adresse alternativ als symbolischen Namen oder numerisch eingeben.

Der Syslog-Server muss vom Security-Modul aus über die angegebene IP-Adresse erreichbar sein, ggf. über die Router-Projektierung im Register "Routing". Wenn der Syslog-Server nicht erreichbar ist, wird das Versenden der Syslog-Informationen abgeschaltet. Sie können diesen Betriebszustand anhand entsprechender Systemmeldungen erkennen. Um das Versenden der Syslog-Informationen erneut zu aktivieren, müssen Sie ggf. die Routing-Informationen aktualisieren und einen Neustart des Security-Moduls veranlassen.

Symbolische Namen im Logging verwenden



Aktivieren Sie das Optionskästchen "Symbolische Namen im Logging verwenden", werden die an den Syslog-Server übermittelten Adressangaben der Log-Telegramme durch symbolische Namen ersetzt. Das Security-Modul prüft, ob entsprechende symbolische Namen projiziert sind und trägt diese in das Log-Telegramm ein.

Hinweis

Höhere Bearbeitungszeit bei symbolischen Namen

Ist das Optionskästchen "Symbolische Namen im Logging verwenden" aktiviert, wird die Bearbeitungszeit im Security-Modul erhöht.

Für die IP-Adressen der Security-Module werden automatisch die Modulnamen als symbolische Namen verwendet. Im Routing-Modus werden diese Namen mit einer Port-Bezeichnung wie folgt erweitert: "Modulname-P1", "Modulname-P2" usw.

Ereignisklassen konfigurieren

Tabelle 8-3 Netzwerk Syslog - Funktionsübersicht

Funktion / Register im Online-Dialog	Projektion	Bemerkungen
Paketfilter-Ereignisse (Firewall)	Die Aktivierung erfolgt über das Optionskästchen. Durch die Einstellung von Facility und Severity lassen sich Syslog-Meldungen entsprechend ihrer Herkunft und ihres Schweregrades klassifizieren. Die Zuordnung erfolgt über Klapplisten. Jedem Ereignis wird die Severity und Facility zugewiesen, die Sie hier einstellen.	Welchen Wert Sie hier wählen, hängt von der Auswertung im Syslog-Server ab. Damit können Sie eine Anpassung an die Erfordernisse im Syslog-Server vornehmen. Lassen Sie den Standardwert "default" eingestellt, wird durch das Security-Modul festgelegt, mit welcher Kombination aus Facility und Severity das Ereignis angezeigt wird.
Audit-Ereignisse	Die Aktivierung erfolgt über das Optionskästchen. Die Zuordnung der Severity und Facility erfolgt über Klapplisten. Jedem Ereignis wird die Severity und Facility zugewiesen, die Sie hier einstellen.	Welchen Wert Sie hier für Severity und Facility wählen, hängt von der Auswertung im Syslog-Server ab. Damit können Sie eine Anpassung an die Erfordernisse im Syslog-Server vornehmen. Lassen Sie den Standardwert "default" eingestellt, wird durch das Security-Modul festgelegt, mit welcher Kombination aus Facility und Severity das Ereignis angezeigt wird.
System-Ereignisse	Die Aktivierung erfolgt über das Optionskästchen.	Zur Konfiguration des Ereignisfilters und der Leitungsdiagnose öffnen Sie über die Schaltfläche "Konfigurieren..." einen weiteren Dialog.

Funktion / Register im Online-Dialog	Projektierung	Bemerkungen
Filterung der System-Ereignisse	Stellen Sie in diesem Sub-Dialog für die Systemereignisse eine Filterebene ein. Standardmäßig sind die folgenden Werte eingestellt: • SCALANCE S: Ebene 0 • CP: Ebene 3	Wählen Sie als Filterebene "Error" oder einen höheren Wert, um die Aufzeichnung von allgemeinen, nicht kritischen Ereignissen abzustellen. Hinweis für CP Wählen Sie für den CP nur Ebene 3 oder Ebene 6 aus. • Bei Auswahl von Ebene 3 werden die Fehlermeldungen der Ebenen 0 bis 3 ausgegeben. • Bei Auswahl von Ebene 6 werden die Fehlermeldungen der Ebenen 0 bis 6 ausgegeben.
Leitungsdiagnose 	Die Leitungsdiagnose erzeugt ein spezielles System-Ereignis. Stellen Sie ein, ab welchem Prozentsatz fehlerhafter Telegramme ein System-Ereignis erzeugt werden soll. Weisen Sie dem System-Ereignis eine Facility und eine Severity zu.	Über die Severity gewichten Sie die System-Ereignisse der Leitungsdiagnose im Verhältnis zur Severity der übrigen System-Ereignisse. Hinweis Weisen Sie den System-Ereignissen der Leitungsdiagnose keine geringere Severity als der Filterung der System-Ereignisse zu. Ansonsten passieren diese Ereignisse den Filter nicht und werden vom Syslog-Server nicht aufgezeichnet.

8.2.3 Projektierung des Paket-Logging

Projektierung des Logging im Standard Modus

Informationen zum Logging von IP- und MAC-Regelsätze finden Sie im Kapitel CPs im Standard Modus (Seite 88) im jeweiligen Unterkapitel des Security-Moduls.

Projektierung des Logging im Erweiterten Modus

Die Aktivierung des Logging ist für beide Regeltypen (IP oder MAC) und alle Regeln identisch. Um Datenpakete bestimmter Paketfilter-Regeln aufzuzeichnen, setzen Sie im Register "Firewall" in der Spalte "Log" einen Auswahlhaken.

Anhang

A.1 DNS-Konformität

DNS-Konformität gemäß RFC1035 beinhaltet folgende Regeln:

- Beschränkung auf 255 Zeichen insgesamt (Buchstaben, Ziffern, Bindestrich oder Punkt);
- der Name muss mit einem Buchstaben beginnen;
- der Name darf nur mit einem Buchstaben oder einer Ziffer enden;
- ein Namensbestandteil innerhalb des Namens, d. h. eine Zeichenkette zwischen zwei Punkten, darf max. 63 Zeichen lang sein;
- keine Sonderzeichen wie Umlaute, Klammern, Unterstrich, Schrägstrich, Blank etc.

A.2 Wertebereiche IP-Adresse, Subnetzmaske und Adresse des Netzübergangs

Wertebereich für IP-Adresse

Die IP-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.80.0.16

Wertebereich für Subnetzmaske

Die Subnetzmaske besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 255.255.0.0

Die 4 Dezimalzahlen der Subnetzmaske müssen in ihrer binären Darstellung von links eine Folge von lückenlosen Werten "1" und von rechts eine Folge von lückenlosen Werten "0" enthalten.

Die Werte "1" bestimmen die Netznummer innerhalb der IP-Adresse. Die Werte "0" die Host-Adresse innerhalb der IP-Adresse.

Beispiel:

richtige Werte:

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

falscher Wert:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

Zusammenhang IP-Adresse und Subnetzmaske

Die erste Dezimalzahl der IP-Adresse (von links) bestimmt den Aufbau der Subnetzmaske hinsichtlich der Anzahl der Werte "1" (binär) wie folgt (für "x" steht die Host-Adresse):

Erste Dezimalzahl der IP-Adresse	Subnetzmaske
0 bis 126	255.x.x.x
128 bis 191	255.255.x.x
192 bis 223	255.255.255.x

Hinweis:

Für die erste Dezimalzahl der IP-Adresse können Sie auch einen Wert zwischen 224 und 255 eintragen. Dies ist jedoch nicht empfehlenswert, da für diese Werte keine Adressprüfung durch STEP 7 erfolgt.

Wertebereich für Adresse des Netzübergangs

Die Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; z. B. 141.80.0.1

Zusammenhang IP-Adresse und Adresse des Netzübergangs

Die IP-Adresse und die Adresse des Netzübergangs dürfen nur an den Stellen unterschiedlich sein, an denen in der Subnetzmaske "0" steht.

Beispiel:

Sie haben eingegeben: für Subnetzmaske 255.255.255.0; für IP-Adresse 141.30.0.5 und für die Adresse des Netzübergangs 141.30.128.0. Die IP-Adresse und die Adresse des Netzübergangs dürfen nur in der 4. Dezimalzahl einen unterschiedlichen Wert haben. Im Beispiel ist aber die 3. Stelle schon unterschiedlich.

Im Beispiel müssen Sie also alternativ ändern:

die Subnetzmaske auf: 255.255.0.0 oder

die IP-Adresse auf: 141.30.128.5 oder

die Adresse des Netzübergangs auf: 141.30.0.0

A.3 MAC-Adresse

Hinweis zum Aufbau der MAC-Adresse:

Die MAC-Adresse besteht aus einem festen und einem variablen Teil. Der feste Teil ("Basis-MAC-Adresse") kennzeichnet den Hersteller (Siemens, 3COM, ...). Der variable Teil der MAC-Adresse unterscheidet die verschiedenen Ethernet-Teilnehmer.

Literaturverzeichnis

B.1 Einleitung

Auffinden der Siemens-Literatur

Die Bestellnummern für Siemens-Dokumentationen sind in den Katalogen "SIMATIC NET Industrielle Kommunikation, Katalog IK PI" und "SIMATIC Produkte für Totally Integrated Automation und Micro Automation, Katalog ST 70" enthalten.

Diese Kataloge sowie zusätzliche Informationen können Sie bei Ihrer Siemens-Vertretung anfordern.

Einige der hier genannten Dokumente finden Sie auch auf der SIMATIC NET Manual Collection, die jedem Gerät beiliegt.

Viele SIMATIC NET-Handbücher finden Sie auf den Internet-Seiten des Siemens Customer Support für Automatisierung.

Link zum Customer Support (<http://support.automation.siemens.com/WW/view/de>)

Geben Sie dort die ID des jeweiligen Handbuchs als Suchbegriff ein. Die ID ist unter einigen Literaturstellen in Klammern angegeben.

Handbücher, die in der Online-Dokumentation der STEP 7-Installation auf Ihrem PG/PC vorhanden sind, finden Sie über das Startmenü ("Start" > "SIMATIC" > "Dokumentation").

Eine Übersichtsseite der SIMATIC-Dokumentation finden Sie im Internet.

Link zur Dokumentation:

(http://www.automation.siemens.com/simatic/portal/html_00/techdoku.htm)

B.2 S7-CPs / Zur Projektierung, Inbetriebnahme und Nutzung des CP

B.2.1 /1/

SIMATIC NET
S7-CPs für Industrial Ethernet
Projektieren und in Betrieb nehmen
Handbuch Teil A - Allgemeine Anwendungen
Projektierungshandbuch
Siemens AG
(SIMATIC NET Manual Collection)
Im Internet unter folgender Beitrags-ID:
30374198 (<http://support.automation.siemens.com/WW/view/de/30374198>)

B.2.2 /2/

SIMATIC NET

S7-CPs für Industrial Ethernet

Handbuch Teil B

Gerätehandbuch

Siemens AG

(SIMATIC NET Manual Collection)

Im Internet finden Sie die Gerätehandbücher für die einzelnen CPs jeweils unter folgender Beitrags-ID:

CP 343-1 Advanced (GX31): 28017299

(<http://support.automation.siemens.com/WW/view/de/28017299>)

CP 443-1 Advanced (GX30): 59187252

(<http://support.automation.siemens.com/WW/view/de/59187252>)

B.3 Zur Projektierung mit STEP 7 / NCM S7

B.3.1 /3/

SIMATIC NET

NCM S7 für Industrial Ethernet

Erste Schritte

Siemens AG

(Bestandteil der Online-Dokumentation in STEP 7)

B.3.2 /4/

SIMATIC NET

PC-Stationen In Betrieb nehmen - Anleitung und Schnelleinstieg

Projektierungshandbuch

Siemens AG

(SIMATIC NET Manual Collection)

Im Internet unter folgender Beitrags-ID:

13542666 (<http://support.automation.siemens.com/WW/view/de/13542666>)

B.3.3 /5/

SIMATIC
Hardware konfigurieren und Verbindungen projektieren mit STEP 7
Siemens AG
(Teil des Dokumentationspakets "STEP 7-Grundwissen")
(Bestandteil der Online-Dokumentation in STEP 7)

B.4 S7-CPs Zur Montage und Inbetriebnahme des CP**B.4.1 /6/**

SIMATIC S7
Automatisierungssystem S7-300

- CPU 31xC und 31x Aufbauen: Betriebsanleitung
Beitrags-ID: 13008499 (<http://support.automation.siemens.com/WW/view/de/13008499>)
- Baugruppendaten: Referenzhandbuch
Beitrags-ID: 8859629 (<http://support.automation.siemens.com/WW/view/de/8859629>)

Siemens AG

sowie

SIMATIC S7
Automatisierungssystem S7-400, M7-400

- Aufbauen: Installationshandbuch
Beitrags-ID: 1117849 (<http://support.automation.siemens.com/WW/view/de/1117849>)
- Baugruppendaten: Referenzhandbuch
Beitrags-ID: 1117740 (<http://support.automation.siemens.com/WW/view/de/1117740>)

Siemens AG

B.5 Zu Aufbau und Betrieb eines Industrial Ethernet-Netzes**B.5.1 /7/**

SIMATIC NET
Handbuch Twisted Pair- und Fiber Optic Netze
Siemens AG
(SIMATIC NET Manual Collection)

B.6 SIMATIC- und STEP 7-Grundlagen

B.6.1 /8/

SIMATIC
Kommunikation mit SIMATIC
Systemhandbuch
Siemens AG
Beitrags-ID:
25074283 (<http://support.automation.siemens.com/WW/view/de/25074283>)

B.6.2 /9/

Dokumentationspaket "STEP 7-Grundwissen"

- Erste Schritte und Übungen mit STEP 7 (ID: 18652511
(<http://support.automation.siemens.com/WW/view/de/18652511>))
- Programmieren mit STEP 7 (ID: 18652056
(<http://support.automation.siemens.com/WW/view/de/18652056>))
- Hardware konfigurieren und Verbindungen projektieren mit STEP 7 (ID: 18652631
(<http://support.automation.siemens.com/WW/view/de/18652631>))
- Von S5 nach S7, Umsteigerhandbuch (ID: 1118413
(<http://support.automation.siemens.com/WW/view/de/1118413>))

Siemens AG
Bestellnummer 6ES7 810-4CA08-8AW0
(Bestandteil der Online-Dokumentation in STEP 7)

B.7 Industrielle Kommunikation Band 2

B.7.1 /10/

SIMATIC NET
Industrial Ethernet Netzhandbuch
Siemens AG
(SIMATIC NET Manual Collection)
Im Internet unter folgender Beitrags-ID: 27069465
(<http://support.automation.siemens.com/WW/view/de/27069465>)

B.8 Zur Konfiguration von PC-Stationen / PGs

B.8.1 /11/

SIMATIC NET
PC-Stationen in Betrieb nehmen - Anleitung und Schnelleinstieg
Projektierungshandbuch
Siemens AG
(SIMATIC NET Manual Collection)
Im Internet unter folgender Beitrags-ID: 13542666
(<http://support.automation.siemens.com/WW/view/de/13542666>)

B.9 Zur Konfiguration von PC-CPs

B.9.1 /12/

SIMATIC NET Industrial Ethernet CP 1628
Kompaktbetriebsanleitung
Siemens AG
(SIMATIC NET Manual Collection)
Im Internet unter folgender Beitrags-ID: 56714413
(<http://support.automation.siemens.com/WW/view/de/56714413>)

B.10 SIMATIC NET Industrial Ethernet Security

B.10.1 /13/

SIMATIC NET Industrial Ethernet Security
SCALANCE S ab V3.0
Inbetriebnahme- und Montagehandbuch
Siemens AG
(SIMATIC NET Manual Collection)
Im Internet unter folgender Beitrags-ID: 56576669
(<http://support.automation.siemens.com/WW/view/de/56576669>)

B.10.2 /14/

SIMATIC NET Industrial Ethernet Security
EDGE/GPRS-Router SCALANCE MD741-1

Systemhandbuch
Siemens AG

(SIMATIC NET Manual Collection)

Im Internet unter folgender Beitrags-ID: 31385703
(<http://support.automation.siemens.com/WW/view/de/31385703>)

B.10.3 /15/

SIMATIC NET
Telecontrol SCALANCE M875

Betriebsanleitung
Siemens AG

(SIMATIC NET Manual Collection)

Im Internet unter folgender Beitrags-ID: 58122394
(<http://support.automation.siemens.com/WW/view/de/58122394>)

Index

*

*.cer, 56, 190
*.dat, 190
*.p12, 56, 70, 190

3

3DES, 172

A

Administrator, 60
Adressband, 121
Adresse des Netzübergangs, 216
Adressparameter, 75
Advanced Encryption Standard (AES), 172
AES, 159, 172
Aggressive Mode, 172
Aktive Teilnehmer, 175
Applet, 64
ARP, 163
ARP-Proxy, 159
Audit-Ereignisse, 207
Authentifizierung, 59
Authentifizierungsmethode, 170
Authentifizierungsmethoden, 164
Autocrossing, 84
Automatische Firewall-Regeln, 112
Autonegotiation, 84

B

Bandbreite, 117, 126
Bedeutung der Symbole, 5
Benutzer
 einrichten, 59
 Rollen anlegen, 60
 Rollen zuweisen, 62
Benutzerdefinierte Rollen, 61
Benutzername, 59
Benutzerrechte, 63
Benutzerspezifische Firewall-Regeln, 110, 125
 Remote-Access Benutzer, 61

Timeout-Parameter, 112
Benutzerspezifische IP-Regelsätze, 111
Benutzerverwaltung, 49, 58
Bridge-Modus, 79
Broadcast, 121, 136

C

CA-Gruppenzertifikat, 70
CA-Gruppenzertifikat erneuern, 175
CA-Zertifikat, 66, 69, 70
Certificate Authority, 66
CHAP, 85
CP 1628
 Aufgabe, 31
CP x43-1 Adv.
 Aufgabe, 27
C-PLUG, 34, 52
CPs anlegen, 74

D

Data Encryption Standard (DES), 173
Datenspionage, 23
Dauerhafte Verbindung, 86
DCP, 105
DCP (Primary Setup Tool), 130
Dead-Peer-Detection (DPD), 176
DES, 159, 173
DHCP
 Server, 104
 Server-Konfiguration, 147
 symbolische Namen, 53
DHCP-Server, 149
Diagnose, 203
Diagnose-Benutzer, 61
Dienstgruppe, 130
Diffie-Hellman-Schlüsselvereinbarung, 172
DNS
 Server, 105
DNS-Konformität, 54, 215
Dynamisches DNS (DynDNS), 80

E

Eigenschaften der VPN-Gruppe, 170
Einstellungen

- projektweite, 49
- Erweiterter Modus, 36
 - Benutzerspezifische Firewall-Regeln, 110
 - DHCP-Server, 149
 - Firewall-Regeln, 106
 - Globale Firewall-Regeln, 107
 - Logging, 214
 - Lokales Logging, 206, 208
 - NAT/NAPT, 135
 - Netzwerk Syslog, 206
- ESP-Protokoll, 90, 96, 172
- eth0, 77
- eth1, 77
- eth2, 77
- Ethernet-Non-IP-Telegramme, 87
- Externe Netzknoten
 - CP x43-1 Adv., 30
 - SCALANCE 602, 22
 - SCALANCE S612/S 623, 26

F

- Facility, 213
- Firewall, 25
 - Erweiterter Modus, 106
 - Firewall-Regeln, 87
 - symbolische Namen, 53
- Firewall aktivieren
 - CP 1628, 88
 - CP x43-1 Adv., 88
 - SCALANCE S < V3.0, 104
 - SCALANCE S V3, 102
- Firewall-Regelsätze
 - benutzerdefinierte, 110
 - globale, 49
- Firewall-Voreinstellung
 - CP 1628, 95
 - CP x43 Adv., 89
 - SCALANCE S < V3.0, 99
- Firmware aktualisieren, 65
- Firmware-Ausgabestand, 4
- Flaches Netz, 79
- FTP, 64
- FTP/FTPS, 46
- FTPS-Zertifikate, 66
- Funktionsübersicht
 - Gerätetypen, 16

G

- Gerätrechte, 63

- Getunnelte Kommunikation aktivieren
 - CP x43-1 Adv., 89
 - SCALANCE S < V3.0, 104
 - SCALANCE S V3, 102
- Gigabit-Adresse, 69
- Globale Firewall-Regeln, 107, 125
 - zuweisen, 109
- Globale Paketfilter-Regeln, 109
- Glossar, 6
- Gruppeneigenschaften, 170
- Gruppennamen, 122, 128
- Gruppenzuordnungen, 49

H

- Halbduplex, 84
- HTTP, 122
- HTTPS, 177

I

- ICMP, 114
- ICMP-Dienste, 124
- IEEE 802.3, 25, 87
- IKE, 90, 96
- IKE-Einstellungen, 170
- Inhaltsbereich, 39, 75
- Installation
 - SCALANCE S, 37
- Interne Netzknoten
 - CP x43-1 Adv., 30
 - konfigurieren, 179
 - SCALANCE 602, 22
 - SCALANCE S612/S 623, 26
- Internet Key Exchange (IKE), 171
- Internet Verbindung, 85
- IP Access Control-Liste, 64
- IP-Adresse, 120, 215
- IP-Dienste, 122
- IP-Paketfilter
 - lokal, 115
- IP-Paketfilter-Regeln, 116
 - CP 1628, 117
 - CP x43-1 Adv., 117
 - SCALANCE S ≥ V3.0, 118
- IP-Protokoll, 106
- IP-Regelsätze, 107
 - benutzerspezifische, 110
- IPsec-Einstellungen, 170
- IPsec-Tunnel, 161
- IP-Verkehr

- mit S7-Protokoll, 104
- vom internen ins externe Netz, 104
- IP-Zugriffsschutz, 46
- ISAKMP, 177
- ISO-Protokoll, 180
- ISP-Account, 85

K

- Konsistenzprüfung, 55, 151
 - lokal, 52
 - projektweit, 53

L

- Layer 2, 87, 106, 163
- Layer 3, 87, 106
- Layer 4, 87
- Lebensdauer von Zertifikaten, 168
- Leitungsdiagnose, 207, 210, 214
- Lernfunktionalität, 179
- Lernmodus, 180
- Linearer Speicher, 207
- LLDP, 64
- Logging, 88, 203
 - CP x43-1 Adv., 89
 - Ereignisklassen, 213
 - SCALANCE S < V3.0, 104
 - SCALANCE S V3, 102
- Lokale Firewall-Regeln, 88
- Lokales Logging, 203, 206, 209
 - Audit-Ereignisse, 209
 - Paketfilter-Ereignisse, 209
 - System-Ereignisse, 210

M

- MAC-Adresse, 79, 216
 - aufgedruckte, 79
 - DMZ, 79
 - im Routing-Modus, 79
 - intern, 79
- MAC-Dienste, 128
- MAC-Paketfilter-Regeln, 124, 126
- MAC-Protokoll, 106
- MAC-Regelsätze, 107
- Main Mode, 172
- MD5, 159, 173
- MD74x, 3, 58
- Mengengerüste, 18
- Menübefehle, 40

- Menüleiste, 40
- MIB, 64
- Mischbetrieb, 165
- Moduleigenschaften, 71
- Multicast, 136

N

- NAT/NAPT
 - Adressumsetzung, 142
 - Konfigurationsbeispiel, 144
 - Routing, 135
- NAT/NAPT-Router
 - symbolische Namen, 53
- Navigationsbereich, 38
- Netz-ID, 134
- Netzknoten
 - Nicht-lernbare, 183
- Netzwerk Syslog, 203, 206
- Non-IP-Telegramme, 163
- NTP (gesichert), 154
- NTP-Server, 104, 154
- NTP-Server exportieren, 157

O

- Offline, 36
- On-Demand Verbindung, 86
- Online, 36
- Online-Diagnose, 205

P

- Paketfilter-Ereignisse, 207
- PAP, 85
- PC-CP, 3
- Perfect Forward Secrecy, 173
- Port
 - 102 (S7-Protokoll - TCP), 122
 - 123 (NTP), 136, 153
 - 20/21 (FTP), 122
 - 443 (HTTPS), 136, 177
 - 4500 (IPsec), 136
 - 500 (IPsec), 136
 - 500 (ISAKMP), 177
 - 514 (Syslog), 136
 - 80 (HTTP), 122
- Preshared Keys, 164
- Produkt von anderem Hersteller, 73
- Produkt-CD SCALANCE S, 37
- PROFINET, 180

PROFINET-Adresse, 69
 Projekt
 Initialisierungswerte, 52
 Projektierungsrechte, 63
 Protokoll, 122
 Puffer, 207

R

Rechteabhängigkeiten, 64
 Remote-Access-Benutzer, 61
 Rollen, 60
 benutzerdefiniert, 61
 systemdefiniert, 60
 Rollenname, 61
 Route anlegen, 134
 Router-IP-Adresse, 134
 Routing aktivieren, 73
 Routing-Modus, 79, 133
 aktivieren, 133
 Rückwirkungsfreiheit, 26

S

S7-CP, 3
 SA-Lebensdauer, 173
 SCALANCE M, 3
 Gruppen-Zertifikat,
 Konfigurationsdatei erstellen,
 Modul-Zertifikat,
 SCALANCE M87x, 3
 SCALANCE S, 3
 Modul anlegen,
 unterstützte Betriebssysteme,
 SCALANCE S602
 Aufgabe, 21
 SCALANCE S612
 Aufgabe, 23
 SCALANCE S623
 Aufgabe, 23
 Schnittstellen, 133
 Schnittstellen-Routing, 78
 Security Configuration Tool, 34, 35, 35
 Bedienungssichten, 36
 Betriebsarten, 36
 in STEP 7, 35, 43
 Installation CP 1628, 37
 Installation CP x34-1 Adv., 37
 Installation SCALANCE S, 37
 Menüleiste, 40
 Standalone, 35, 43

Security-Einstellungen, 187
 Security-Modul, 3
 Severity, 213
 SHA1, 173
 SHA-1, 159
 SiClock, 130
 SiClock-Uhrzeittelegramme, 105
 SIMATIC NET DVD, 37
 SIMATIC NET Glossar, 6
 SNMP, 64
 SNMPv1, 159
 SNMPv3, 159
 SOFTNET Security Client, 3
 Anlaufverhalten, 189
 Aufgabe, 20
 Datenbasis, 190
 deinstallieren, 189
 im Projekt konfigurieren, 189
 Konfigurationsdatei erstellen, 189
 Lernen der internen Knoten, 198
 unterstützte Betriebssysteme, 187
 Spezifizierte Verbindungen, 45, 47, 87
 SSL-Zertifikat, 69
 Stammzertifizierungsstellen, 68
 Standard Modus, 36
 Firewall, 88
 Logging, 214
 Lokales Logging, 206
 Standard-Benutzer, 60
 Standard-Initialisierungswerte, 52
 Standard-Router, 75, 134
 Stateful Packet Inspection, 87
 Statuszeile, 39
 STEP 7, 43
 Benutzermigration,
 migrierte Daten, 44
 Objekteigenschaften,
 Subnetzmaske, 75, 215
 Symbole, 5
 Symbolische Namen, 53, 212
 Symboltabelle, 54
 Syslog
 Audit-Ereignisse, 213
 Paketfilter-Ereignisse, 213
 symbolische Namen, 53
 System-Ereignisse, 213
 Syslog-Server, 50, 203, 211
 Systemdefinierte Rolle
 administrator, 60
 diagnostics, 61
 remote access, 61
 standard, 60

System-Ereignisse, 207

T

TCP, 114, 122, 144

Teilnehmer mit unbekannter IP-Adresse, 174

Tunnel, 161

Tunnel-Funktionalität, 161

U

UDP, 114, 122, 144, 153

Uhrzeitführung konfigurieren, 154

Umlaufspeicher, 207

Unknown Peers, 174

Unspezifizierte Verbindungen, 45, 47

Unterstützte Betriebssysteme

 SCALANCE S, 37

 SOFTNET Security Client, 187

V

Verbindungsdetails, 168

Verbindungsregeln, 113

Verschlüsselung, 36, 52

VLAN-Betrieb, 164

VLAN-Tagging, 164

Vordefinierte Firewall-Regeln

 CP x43-1 Adv., 88

 SCALANCE S < V3.0, 104

 SCALANCE S V3, 102

Vorschaubereich, 39

VPN, 20, 161

 modulspezifische Eigenschaften, 176

 SOFTNET Security Client, 185

VPN Client, 73

VPN-Gruppe, 166

W

WAN IP-Adresse

 auswählen, 168

WAN-IP-Adresse

 festlegen, 177

Wertebereich für IP-Adresse, 215

Z

Zeitsynchronisierung, 154

Zertifikat, 67, 164

 austauschen, 70

 durch Zertifizierungsstelle signiert, 69

 erneuern, 68

 ersetzen, 70

 exportieren, 66

 importieren, 66

 selbst-signiert, 69

Zertifikatsmanager, 67

Zertifizierungsstelle, 67

Zugriffsschutz, 34

